

CT-Router GPRS / UMTS



Benutzerhandbuch

Copyright © comtime GmbH

comtime GmbH
Gutenbergring 22
22848 Norderstedt
Germany

Tel: +49 (0)40 55 44 89 40
Fax: +49 (0)40 55 44 89 45

Internet: http://www.comtime-com.de
email: support@comtime-com.de

Technische Änderungen vorbehalten.

Alle Lieferungen und Leistungen erbringt die comtime GmbH auf der Grundlage der Allgemeinen Geschäftsbedingungen der comtime GmbH in der jeweils aktuellen Fassung. Alle Angaben basieren auf Herstellerangaben. Keine Gewähr oder Haftung bei fehlerhaften und unterbliebenen Eintragungen. Die Beschreibungen der Spezifikationen in diesem Handbuch stellen keinen Vertrag da.

Produkt-Nr.: UMTS 229-01
GPRS 228-00

Inhalt

Inhalt

Technische Daten

Versorgung	
Versorgungsspannung	10V DC … 30V DC über steckbare Schraubklemme
Nennstromaufnahme	< 200mA bei 24V, < 580mA bei 10V
Standby-Stromaufnahme	< 90mA bei 24V
LED-Anzeige	Power (LED grün), Dauerlicht: Betrieb

Schnittstelle	
Netzschnittstelle	
UMTS Frequenzen	850 MHz, 1900 MHz, 2100 MHz (UMTS/HSPA)
Sendeleistung	0,25 W
UMTS-Kompatibilität	UMTS/HSPA 3GPP Release 6 HSUPA max. 5.76Mbps HSDPA max. 7.2Mbps
SIM-Schnittstelle	2 Schnittstellen, 1,8 Volt und 3-Volt-SIM-Karte
GSM Frequenzen	850 MHz, 900 MHz, 1800 MHz, 1900 MHz (GPRS/EDGS)
Sendeleistung	Max. 2,0 W
GPRS-Kompatibilität	GPRS Class 12, Class B, Codierungsschema: CS1 ... CS4
EDGE	EDGE (E-GRPS) Multislot Class 10
Antennenanschluss	50 Ω Impedanz SMA-Antennenbuchse
LED	SIM (LED grün),NET (LED Bargraph)
Ethernet-Schnittstelle	
Anschlussart	RJ45-Buchse, geschirmt
Übertragungsrate	10/100 MBit/s
Unterstützte Protokolle	TCP/IP, UDP/IP, FTP, HTTP
Hilfsprotokolle	ARP, DHCP, PING(ICMP), SNMP V1, SMTP
LED-Anzeige / Steuer-signalindikator	ACT (LED gelb), Ethernet-Datenübertragung LINK (LED grün), Ethernet-Link hergestellt
Serielle-Schnittstelle	
optional	
I/O	
4 Eingänge, 4 Ausgänge über steckbare Schraubklemme	

Technische Daten

Physikalische Merkmale	
Größe (HxBxT)	101 mm x 116 mm x 23 mm
Umgebungstemperatur	Betrieb -25°C...+60°C, Lagerung -40°C …+75°C
Luftfeuchtigkeit	0...95% (nicht kondensierend)
Schutzart	IP20

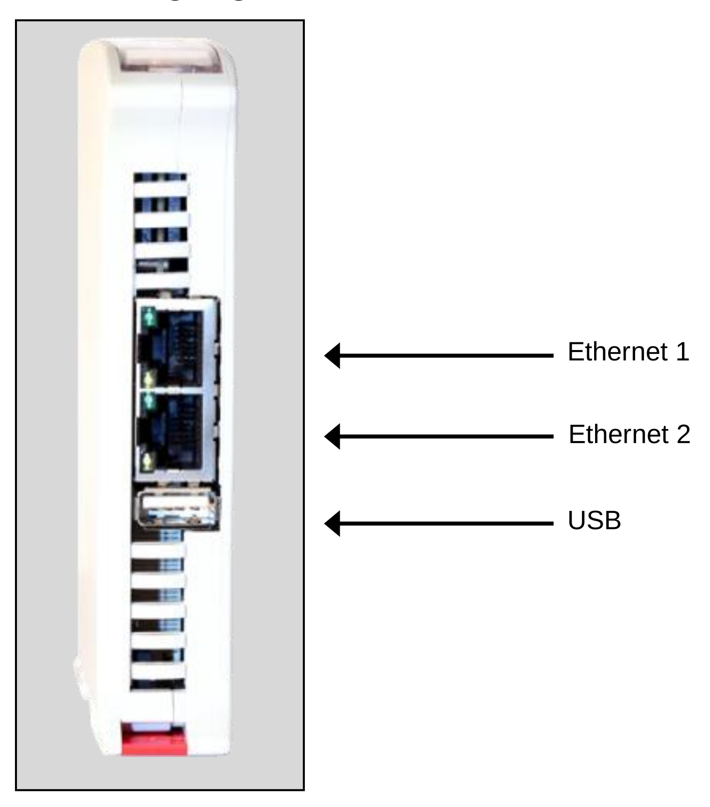
CE-Konformität gemäß R&TTE-Richtlinie 1999/5/EG	
EMV	EN 61000-6-2, EN55022 Class B
Sicherheit	EN 60950
Funk	EN 301511

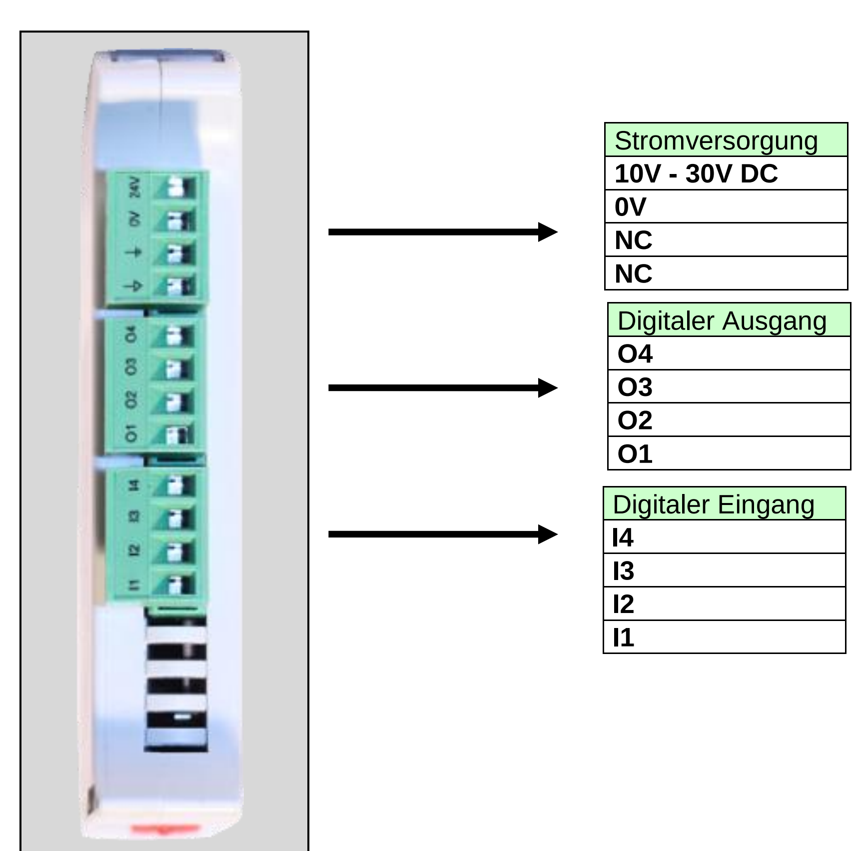
Zulassungen	
UL, USA / Kanada	in Bearbeitung

Technische Änderungen vorbehalten!

Hardware Installation

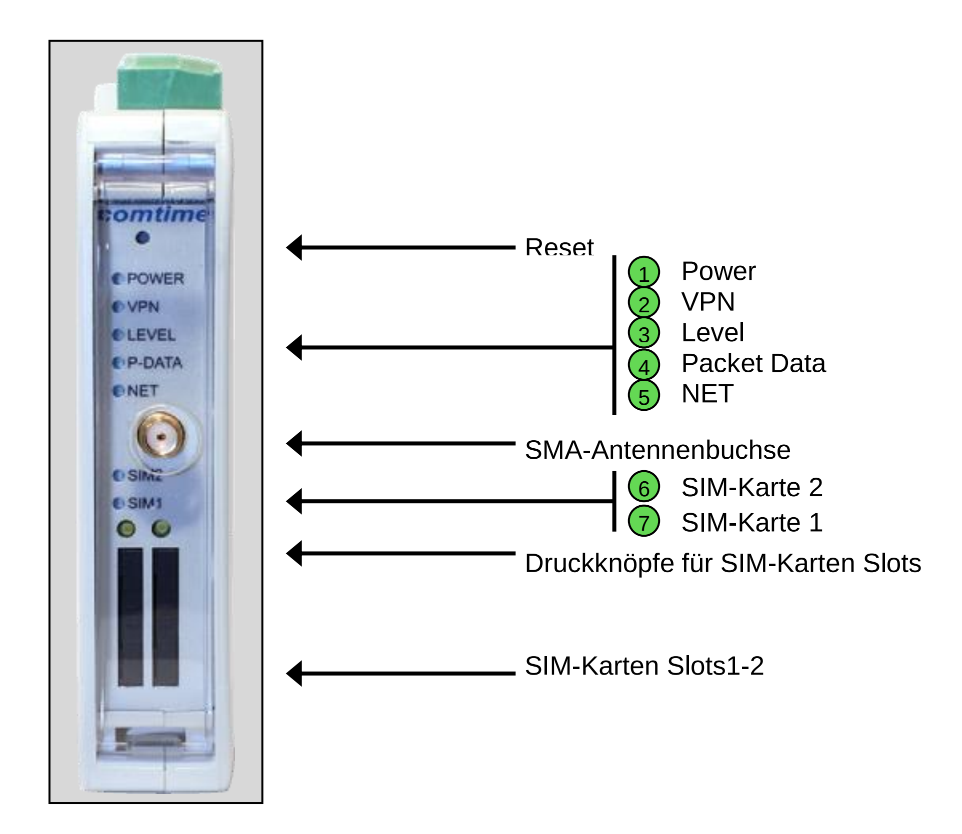
Anschlussbelegung





Hardware Installation

LED Anzeigen



LED Router HSPA	
LED	**Erklärung**
SIM-Karte 1/2	Aus = keine SIM-Karte Ein = SIM / PIN ok schnelles Blinken = falsche PIN langsames Blinken = keine PIN
NET	Aus = nicht eingebucht Blinken = GPRS/EDGE Ein = UMTS/HSDPA/HSUPA
Packet Data	Aus = keine Verbindung Blinken = Modem Verbindung Ein = Paketdaten-Verbindung
Level	Aus = nicht eingebucht Blinken: kurz Ein - lang Aus = -109dBm … -89dBm Blinken: lang Ein - kurz Aus = -87dBm … -67dBm Ein = -65dBm … -51dBm oder besser
VPN	Aus = keine VPN-Verbindung Ein = VPN-Verbindung aktiv
Power	Aus = keine Stromversorgung Ein = Stromversorgung aktiv

Konfiguration WBM

Die Konfiguration des CT-Router HSPA erfolgt über eine Webbrowser basierende Funktion. Hierfür müssen zunächst folgende Bedingungen erfüllt sein:

- Der Computer, der zur Konfiguration des Routers verwendet wird, verfügt über eine LAN-Schnittstelle.
- Auf dem Computer ist ein Webbrowser installiert (z.B. Google Chrome, Mozilla Firefox, Microsoft Internet Explorer).
- Der Router ist mit einer Spannungsquelle verbunden.

Start der Konfiguration

1. Ethernet-Verbindung zwischen Computer und Router herstellen.
2. IP-Adresse der LAN-Schnittstelle auf das Netz des Routers abstimmen.
3. Webbrowser öffnen.
4. Die IP-Adresse des Routers (192.168.0.1) in das Adressfeld des Browsers eingeben und mit Eingabe bestätigen. Anschließend wird eine Benutzername/Passwort-Abfrage erfolgen.



Im Auslieferungszustand lautet der Benutzername „admin“ und das Passwort „admin“ (das Ändern des Passwortes wird im späteren Verlauf beschrieben).
Des Weiteren gibt es zwei User-Level:

- User: Lesezugriff auf „Device Information“
- Admin: Lese- und Schreibzugriff auf alle Bereiche

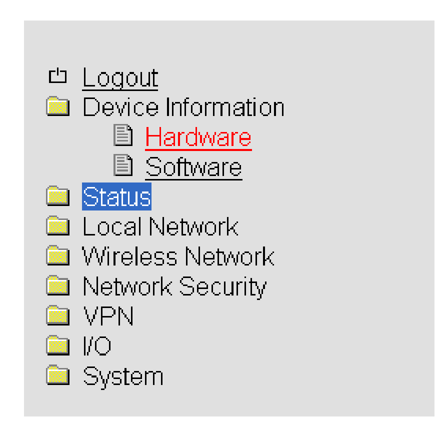
Nach der Eingabe des Benutzernamens und des Passwortes öffnet sich das Hauptmenü zur Konfiguration des CT-Router HSPA.



Device Information

In diesem Bereich können Sie genauere Informationen zur eingebauten Hardware, sowie der installierten Software einsehen.

Hardware



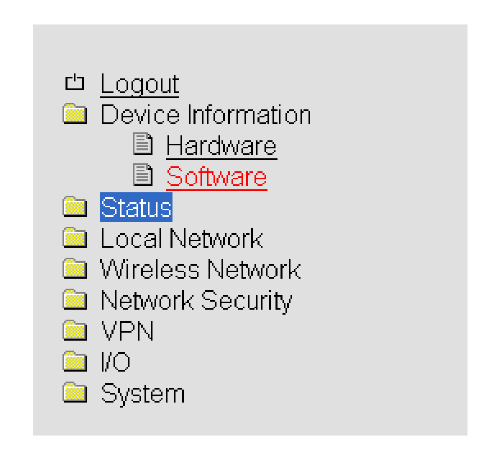
CT-Router HSPA

Hardware Information	
Address	comtime GmbH 22848 Norderstedt Germany
Internet	www.comtime-com.de
Type	CT-Router HSPA
Order-No.	229-01
Serial Number	2000010001
Hardware	Rev: A virtual
Release Version	1.01.2
Operating System	Linux 3.2.0-4-amd64
Web Based Management	1.36.10
MAC Address LAN1	8C-89-A5-61-93-E4
MAC Address LAN2	
Radio-Engine	PH8-P
Radio-Firmware	REVISION 02.002
IMEI	112233445566778

Tabellarische Übersicht der eingebauten Hardware.

Device Information

Software



CT-Router HSPA

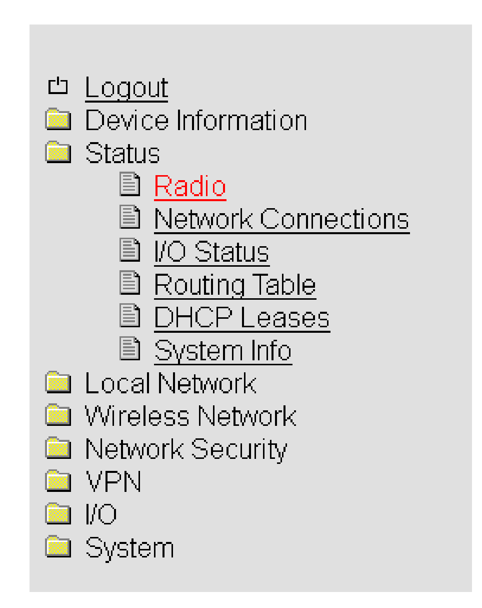
Software Information	
alertsd	0.71.3
busybox	1.18.5-1.6
conchkd	0.30.2
dnsmasq	2.57-1.2
dropbear	0.53.1-1.6
ez-ipupdate	3.0.11b8-1.0
gsmCtrld	3.5.8
inputsd	0.13.3
iproute2	2.6.38-1.3
ipsec	2.8.11-2.0
iptables	1.4.10-1.1
liboping	0.5.1-1.1
msmtp	1.4.27-1.0
netplug	1.2.9-1.2
openntpd	3.10p2-1.1
openssl	1.0.0k
openvpn	2.2.2-1.1
portmap	6.0-1.2
pppd	2.4.5-1.6
watchdog	0.16.3

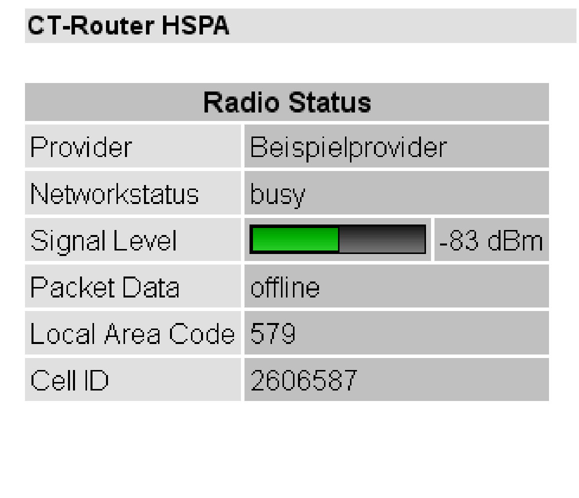
Tabellarische Übersicht der auf dem CT-Router HSPA installierten Software.

Status

In diesem Menü werden Ihnen aktuelle Status-Informationen zum GSM-Netz und Netzwerkverbindungen angezeigt.

Radio





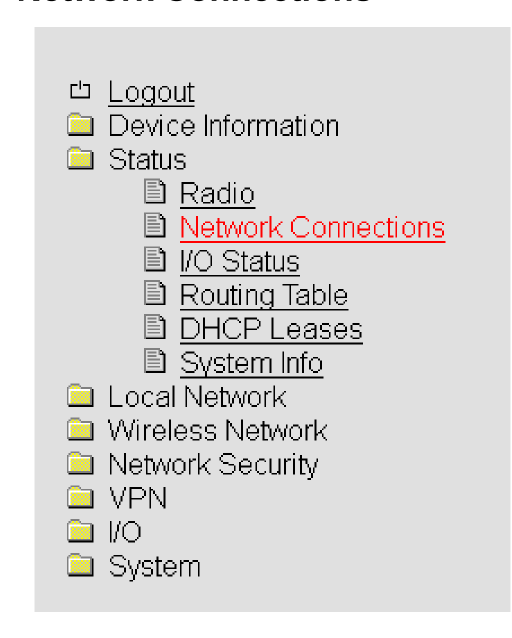
Status >> Radio	
Provider	Providername
Networkstatus	**Registered home:** Einwahl im heimatlichen Mobilfunknetz **Roaming:** Einwahl in das Mobilfunknetz über einen fremden Provider **Waiting for PIN:** es ist noch keine PIN-Eingabe erfolgt **Waiting for PUK:** PIN wurde drei Mal falsch eingegeben, PUK erforderlich **Wrong PIN:** falsche PIN-Eingabe **No SIM Card:** es ist keine SIM-Karte vorhanden **Power off:** GSM-Modul nicht bereit
Signal Level	Signalstärke des Netzes (dBm-Wert)

Status

Packet Data	**offline:** Paketdaten-Verbindung nicht aufgebaut **GPRS online:** Aktive Paketdaten-Verbindung, GPRS-Signal **EDGE online:** Aktive Paketdaten-Verbindung, EDGE-Signal **UMTS online:** Aktive Paketdaten-Verbindung, UMTS-Signal **HSDPA/UPA online:** Aktive Paketdaten-Verbindung, HSDPA/UPA-Signal
Local Area Code	Gebietskennzahl des Mobilfunknetzes
Cell ID	ID der Mobilfunkzelle

Status

Network Connections



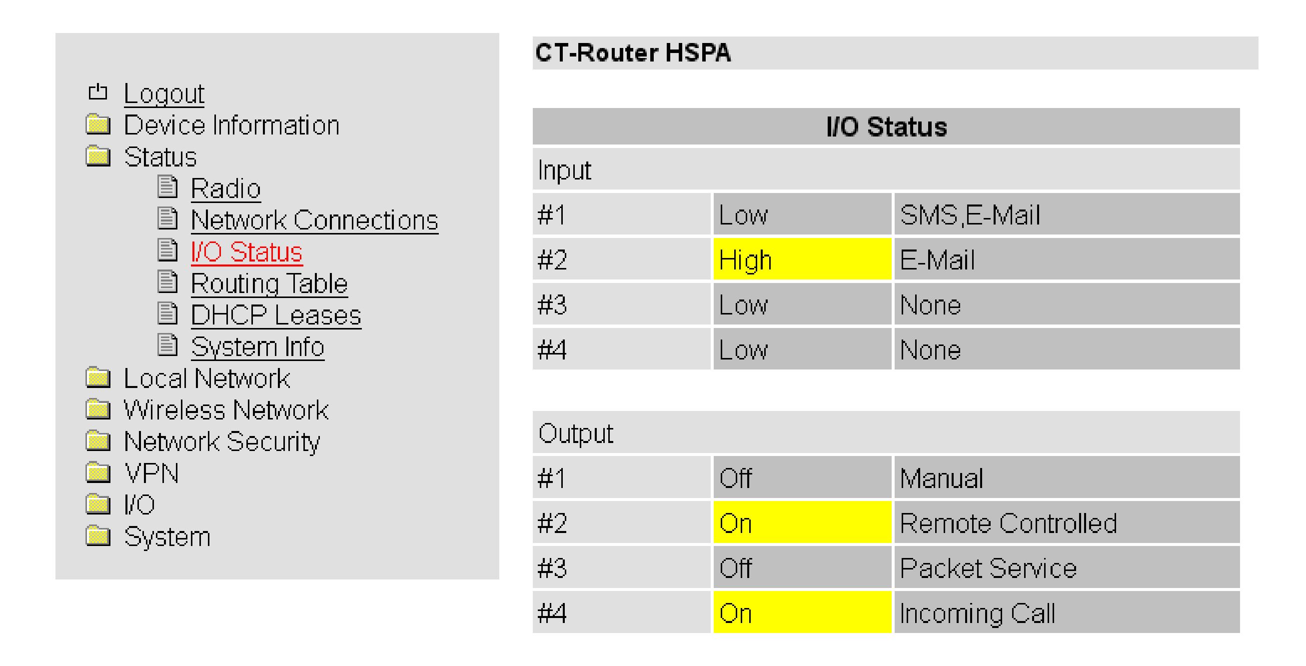
CT-Router HSPA

Network Connections	
Wireless Network	
Link	not connected
Local Network	
Link	connected
IP Address	85.214.27.44
Netmask	255.255.255.255
IP Address Alias(1)	85.214.242.129
Netmask Alias(1)	255.255.255.255

Status >> Network Connections	
Wireless Network	
Link	**TCP/IP connected:** TCP/IP Verbindung im Mobilfunknetz aufgebaut. **VPN connected:** VPN Verbindung im Mobilfunknetz aufgebaut. **not connected:** Es besteht keine aktive Verbindung im Mobilfunknetz.
IP Address	zugewiesene IP-Adresse (Providervorgabe)
Netmask	zugewiesene Netzmaske (Providervorgabe)
DNS Server	DNS-Server IP-Adresse
Sec. DNS Server	alternative DNS-Server IP-Adresse
RX Bytes	Anzahl der empfangenen Daten seit Login in das Mobilfunknetz in Bytes.
TX Bytes	Anzahl der gesendeten Daten seit Login in das Mobilfunknetz in Bytes.
Local Network	
Link	**connected:** Lokale Ethernet-Verbindung aufgebaut **not connected:** keine lokale Ethernet-Verbindung aufgebaut
IP Address	Ethernet IP-Adresse
Netmask	Ethernet Netzmaske

Status

I/O Status

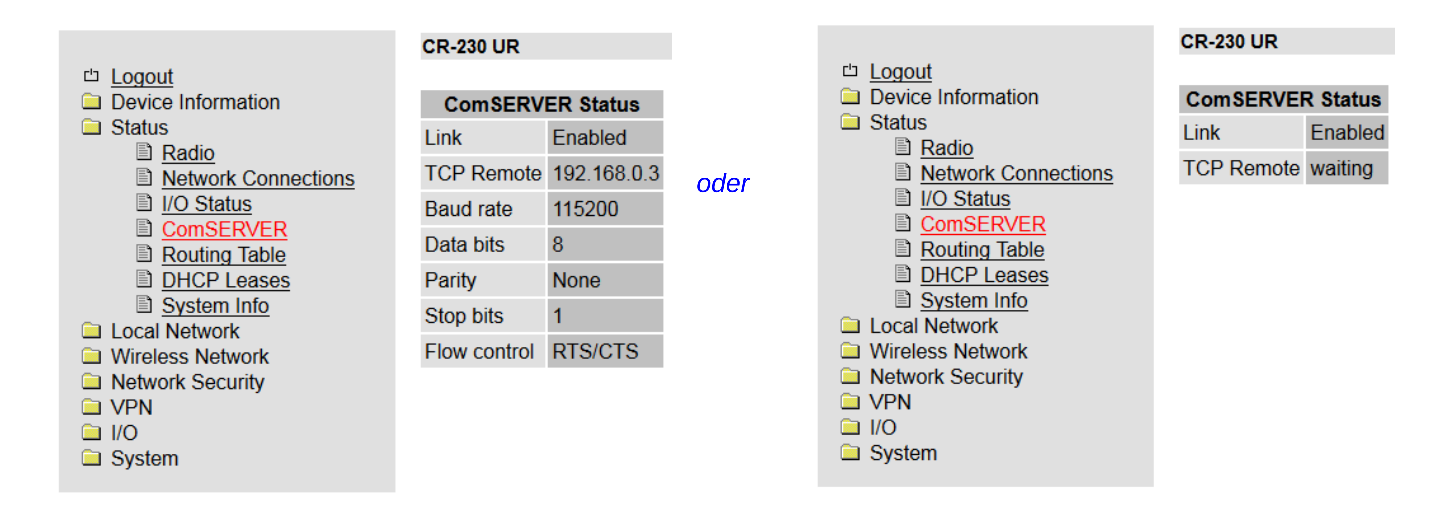


I/O Status		
Input		
#1	Low	SMS,E-Mail
#2	High	E-Mail
#3	Low	None
#4	Low	None
Output		
#1	Off	Manual
#2	On	Remote Controlled
#3	Off	Packet Service
#4	On	Incoming Call

Tabellarische Übersicht aller aktuellen Input- und Outputeinstellungen.

Status

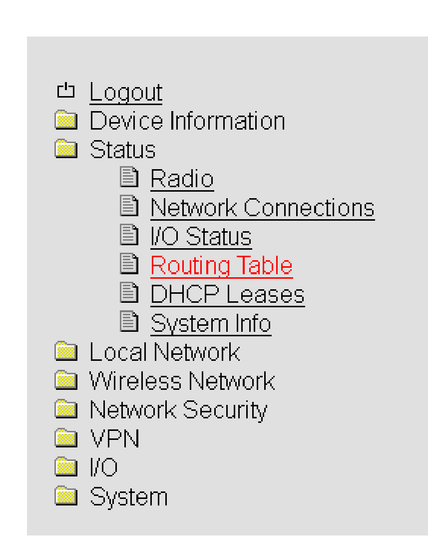
ComSERVER – Status (optional)



Status >>ComSERVER	
Link	Hier wird der Status der ComSERVER (seriellen) Verbindung angezeigt:
TCP Remote	
Baud Rate	
Data bits	
Parity	
Stop bits	
Flow control	

Status

Routing Table



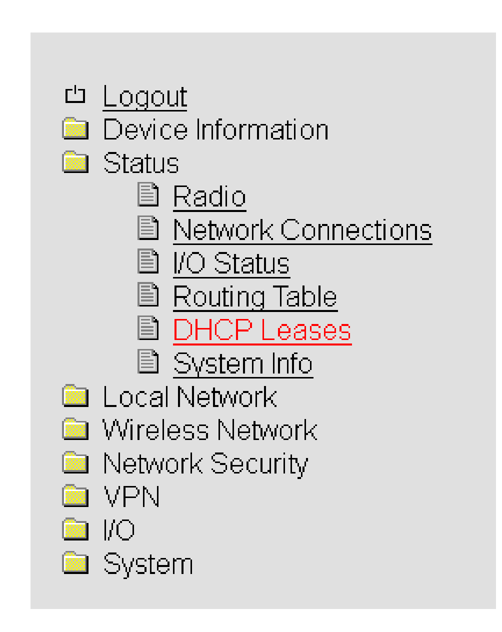
CT-Router HSPA

Kernel IP routing table							
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	85.214.26.1	0.0.0.0	UG	0	0	0	eth0
10.8.0.0	10.8.0.2	255.255.255.0	UG	0	0	0	tun2
10.8.0.2	0.0.0.0	255.255.255.255	UH	0	0	0	tun2
10.11.0.0	10.11.0.2	255.255.255.0	UG	0	0	0	tun1
10.11.0.2	0.0.0.0	255.255.255.255	UH	0	0	0	tun1
10.142.0.0	10.142.0.2	255.255.255.0	UG	0	0	0	tun0
10.142.0.2	0.0.0.0	255.255.255.255	UH	0	0	0	tun0
85.214.26.1	0.0.0.0	255.255.255.255	UH	0	0	0	eth0

Status >>Routing Table
Enthält unter anderen Informationen zum Ziel, Gateway, zur Subnetzmaske und Metrik.

Status

DHCP Leases



CT-Router HSPA

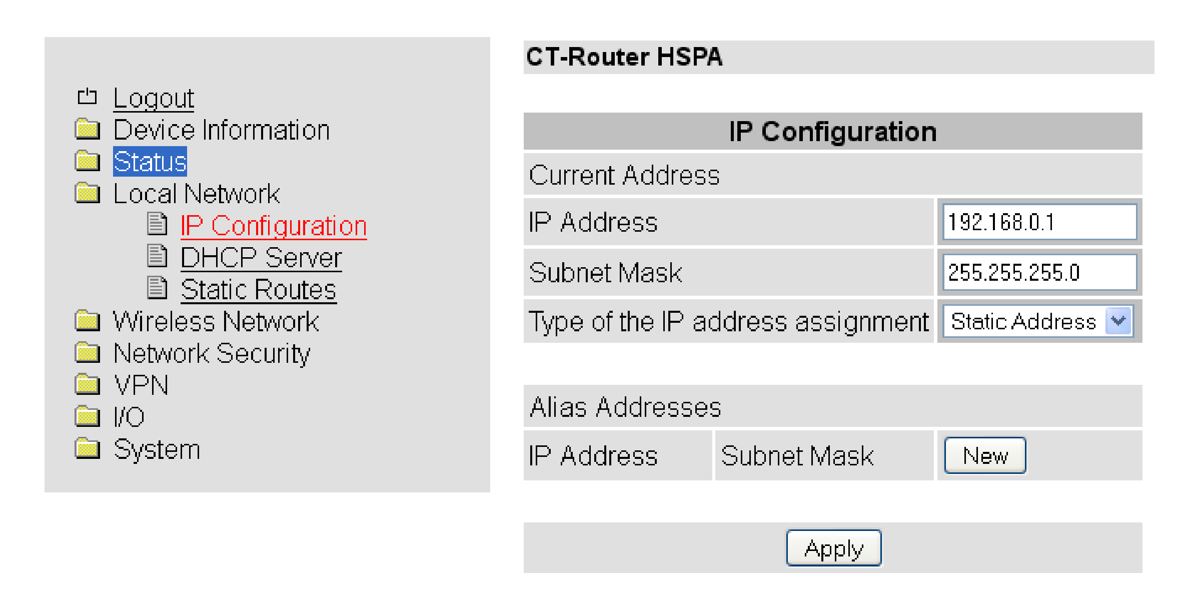
DHCP Leases		
Host Name	Client MAC Address	Client IP Address
raspberrypi	B8-27-EB-75-F1-CE	192.168.2.102
thinkpad	00-16-6F-81-47-B2	192.168.2.105
DMP117	00-05-CD-13-9E-2F	192.168.2.117
Vbox8	08-00-27-48-75-8D	192.168.2.127
S685-IP	7C-2F-80-15-62-D5	192.168.2.129

Status >>DHCP Leases	
Tabellarische Übersicht aller vom CT-Router HSPA vergebenen DHCP-Daten.	
Host Name	Hostname des im Netzwerk befindlichen Endgerätes
Client MAC Address	MAC-Adresse des im Netzwerk befindlichen Endgerätes
Client IP Address	IP-Adresse des im Netzwerk befindlichen Endgerätes

Local Network

Im Menü „Local Network“ können Sie die lokale Netzwerkeinstellung für den CT-Router HSPA vornehmen.

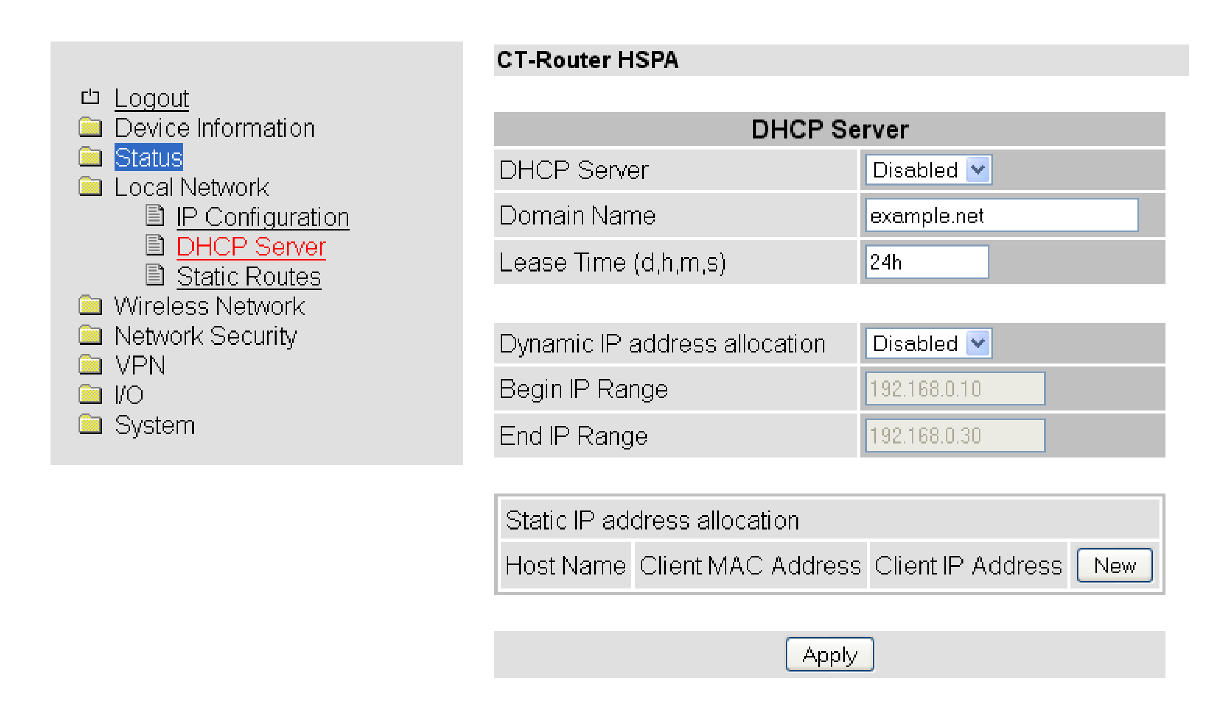
IP Configuration



Local Network >> IP Configuration	
Current Address	
IP Address	aktuelle IP-Adresse des Routers
Subnet Mask	Subnetzmaske der aktuellen IP-Adresse
Type of the IP address assignment	**Static:** Statische IP-Adresse (Standardeinstellung) **DHCP:** Dynamische IP-Adresse, wird beim Start des Routers von einem DHCP-Server bezogen
Alias Addresses	Max. 8 zusätzliche IP-Adressen sowie Subnetzmasken zuweisbar.
IP Address	alternative IP-Adresse des Routers
Subnet Mask	alternative Subnetzmaske des Routers

Local Network

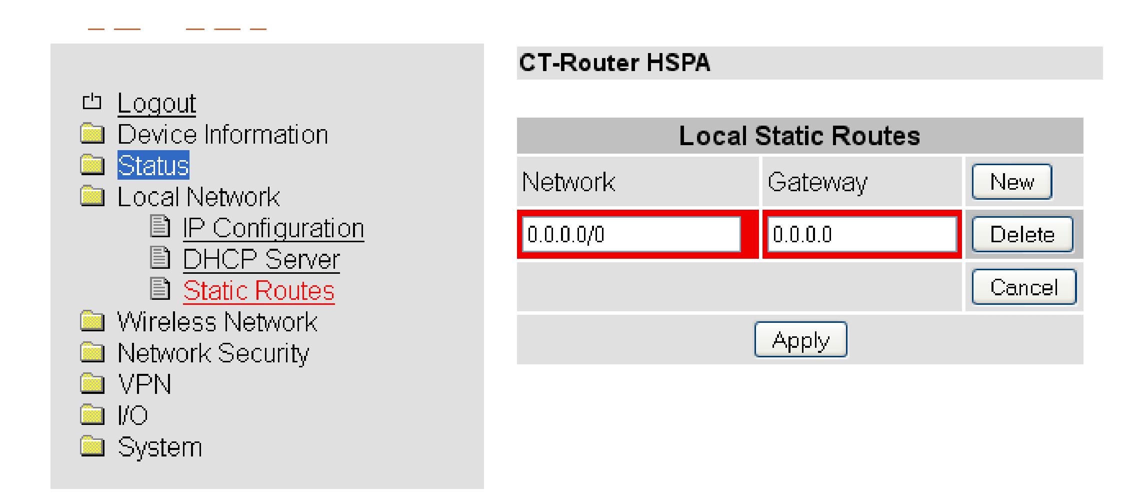
DHCP Server



Local Network >> DHCP Server	
DHCP Server	Deaktiviert / Aktiviert
Domain Name	Domain-Namen eintragen, der über DHCP verteilt wird.
Lease Time (d,h,m,s)	Zeitraum, in dem die Netzwerkkonfigurationen gültig sind.
Dynamic IP address allocation	Dynamische IP-Adressen-Zuweisung: Bei Aktivierung können Sie die entsprechenden Netzwerkparameter eintragen / Der DHCP-Server vergibt IP-Adressen aus dem angegeben IP-Bereich.
Begin IP Range	IP-Bereichsanfang
End IP Range	IP-Bereichsende
Static IP address allocation	IP-Adressen werden MAC-Adressen eindeutig zugeordnet.
Client MAC Address	MAC-Adresse des verbundenen Endgerätes
Client IP Address	IP-Adresse des verbundenen Endgerätes IP-Adressen dürfen nicht aus den dynamischen IP-Adressen Zuweisungen stammen. Eine IP-Adresse darf nicht mehrfach zugeordnet werden, da sonst einer IP-Adresse mehreren MAC-Adressen zugewiesen wird.

Local Network

Static Routes

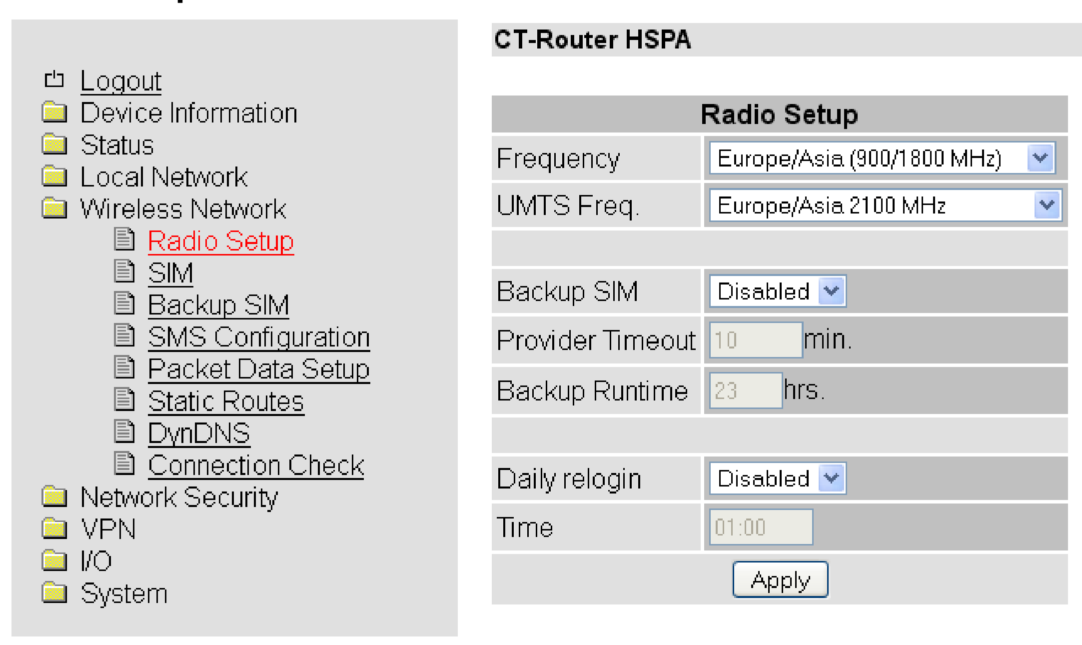


Local Network >> Static Routes	
Network	Netzwerk in CIDR-Form
Gateway	Gateway-Adresse des Netzwerkes
Max. 8 Netzwerke eintragbar.	

Wireless Network

Im “Wireless Network”-Menü legen Sie Einstellungen für die Nutzung des Mobilfunknetzwerkes des Router HSPA fest.

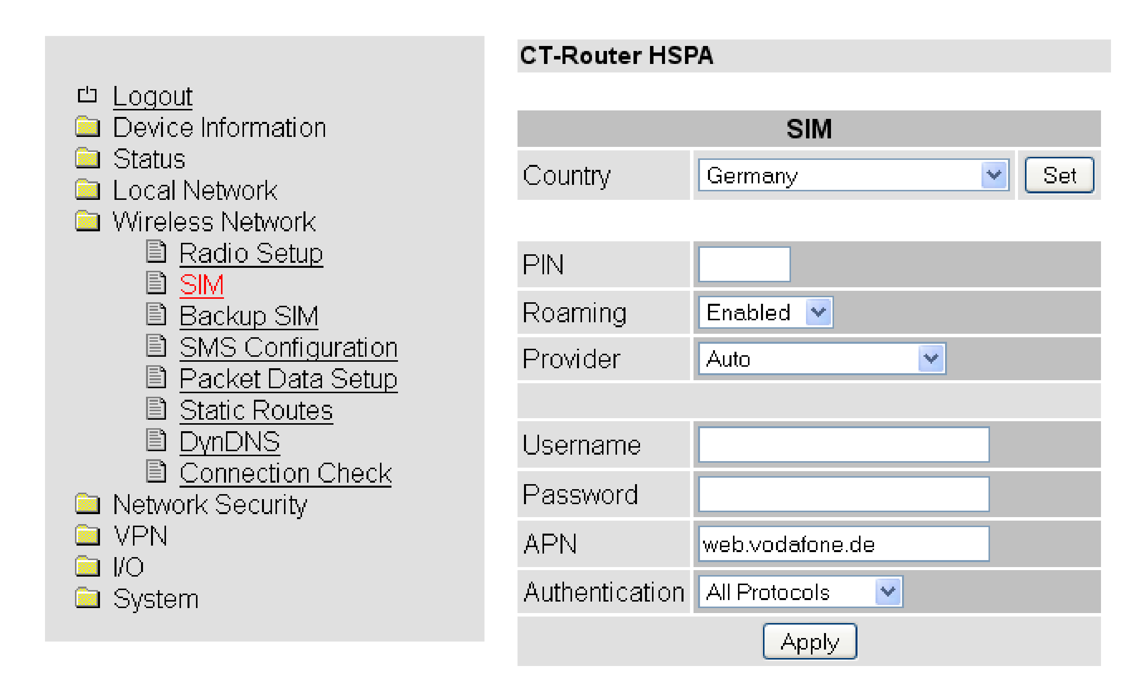
Radio Setup



Wireless Network >> Radio Setup	
Frequency	Frequenzbereich des Routers mithilfe einer Dropdown-Liste auswählen.
UMTS Freq.	Frequenzbereich für UMTS mithilfe einer Dropdown-Liste auswählen / UMTS kann auch deaktiviert werden.
Backup SIM	Zweite SIM-Karte kann für eine Backup-Mobilfunkverbindung genutzt werden.
Provider Timeout	Zeit in Minuten für Aktivierung der Backup-SIM-Karte nach Ausfall der Primären.
Backup Runtime	Laufzeit in Stunden der zweiten SIM-Karte
Daily relogin	**Disable:** Deaktivierung des täglichen Logins **Enable:** Aktivierung des täglichen Logins (Primär vor Sekundär SIM)
Time	Zeitpunkt der Neuanmeldung des Routers in das Mobilfunknetz (Es erfolgt zunächst eine Abmeldung. Bei Neuanmeldung Primär vor Sekundär SIM).

Wireless Network

SIM



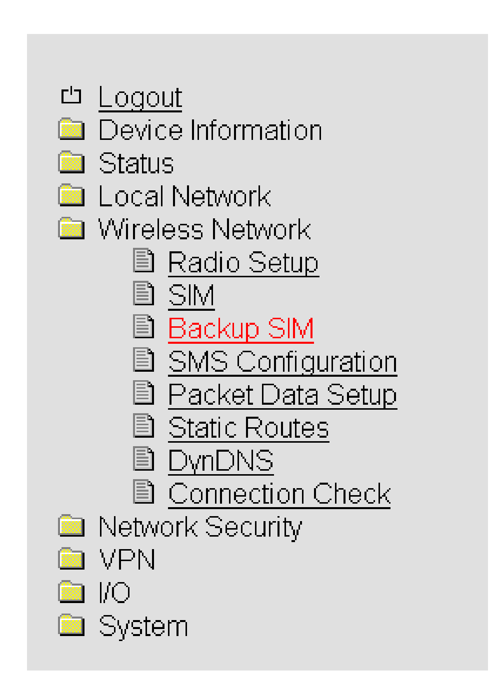
Wireless Network >> SIM	
Country	Auswahl des Landes, in dem der Router in das GSM-Netz eingewählt wird. (Schränkt die Auswahl unter dem Punkt "Provider" ein.)
PIN	PIN-Eingabe der SIM-Karte
Roaming	**Enable:** Es besteht die Möglichkeit, dass der Router sich über ein fremdes Netz einwählen kann. Hierbei können je nach Vertrag zusätzliche Kosten entstehen.
	Disable: Deaktivierung des Roamings. Es wird automatisch das Heimatnetz des Providers genutzt. Sollte dies nicht möglich sein, kommt keine Verbindung zustande.
Provider	Nur wenn das Roaming aktiviert ist, ist eine Auswahl möglich. **Auto:** Automatische Auswahl des Providers
Username	Benutzernamen für Paketdaten-Zugang (Providervorgabe)
Password	Passwort für Paketdaten-Zugang (Providervorgabe)
Benutzername und Passwort immer angeben, da sonst keine Paketdaten-Verbindung zustande kommt.	
APN	Name des Anschlusspunktes im Paketdaten-Netzwerk (Providervorgabe)

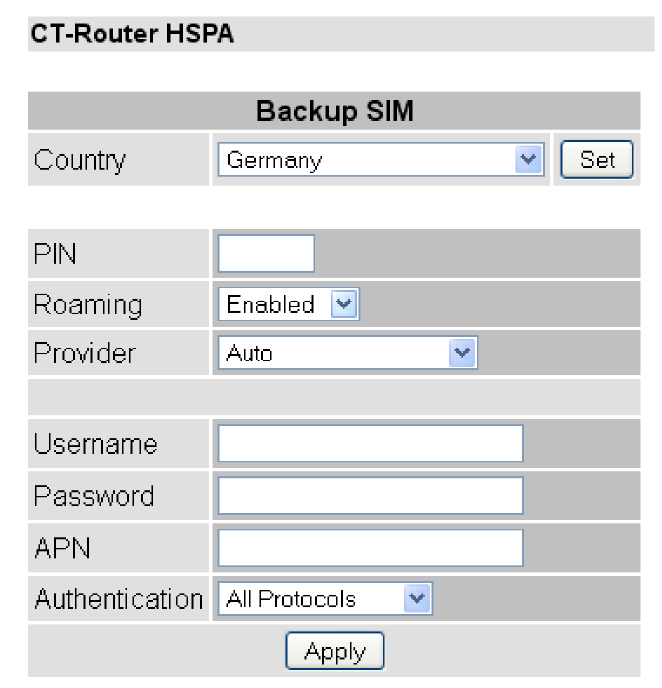
Wireless Network

Authentication	Authentifizierung wird durch Protokolle geschützt. **All Protocols:** Alle Protokolle sind erlaubt **refuse MSCHAP:** Ablehnung des Microsoft Challenge-Handshake Authentication Protocol. **CHAP only:** Nur Challenge-Handshake Authentication Protocol **PAP only:** Nur Password Authentication Protocol

Wireless Network

Backup SIM





Wireless Network >> Backup SIM	
Country	Auswahl des Landes, in dem der Router in das GSM-Netz eingewählt wird (Schränkt die Auswahl unter dem Punkt "Provider" ein.)
PIN	PIN-Eingabe der SIM-Karte
Roaming	**Enable:** Es besteht die Möglichkeit, dass der Router sich über ein fremdes Netz einwählen kann. Hierbei können je nach Vertrag zusätzliche Kosten entstehen. **Disable:** Deaktivierung des Roamings. Es wird automatisch das Heimatnetz des Providers genutzt. Sollte dies nicht möglich sein, kommt keine Verbindung zustande.
Provider	Nur wenn das Roaming aktiviert ist, ist eine Auswahl möglich. **Auto:** Automatische Auswahl des Providers
Username	Benutzernamen für Paketdaten-Zugang (Providervorgabe)
Password	Passwort für Paketdaten-Zugang (Providervorgabe)
Benutzername und Passwort nicht leer lassen, da sonst keine Paketdaten-Verbindung zustande kommt.	
APN	Name des Anschlusspunktes im Paketdaten-Netzwerk (Providervorgabe)
Authentication	Authentifizierung wird durch Protokolle geschützt.
	All Protocols: Alle Protokolle sind erlaubt
	refuse MSCHAP: Ablehnung des Microsoft Challenge-Handshake Authentication Protocol.
	CHAP only: Nur Challenge-Handshake Authentication Protocol
	PAP only: Nur Password Authentication Protocol

Wireless Network

SMS Configuration

Steuerung des Mobilfunkrouters per SMS
Klicken unter „SMS Control" auf Enable. Definieren Sie zum Schutz ein SMS-Passwort.
Das Passwort kann bis zu 7 alphanumerische Zeichen enthalten.

SMS-Syntax
Die Steuerung erfolgt nach folgender SMS Syntax:

#<password>:<command>
<password> = ('A'-'Z', '0'-'9') // bis zu 7 alphanumerische Zeichen

<command> = SET:<sub_cmd> // set command (ON)
<command> = CLR:<sub_cmd> // clear command (OFF)
<sub_cmd> = OUTPUT // output set to ON/OFF
<sub_cmd> = IPSEC // IPsec VPN 1 ON/OFF
<sub_cmd> = IPSEC:n // IPsec VPN n ON/OFF, n={1..x}

<command> = SEND:STATUS // send a status SMS to the caller
<command> = RESET // reset all alarms
<command> = REBOOT // Reboot des Routers

Beispiel:
Einschalten des Outputs der I/O-Schnittstelle. Das (Beispiel-)Passwort lautet: „ct12345".
Die SMS an die Rufnummer des Routers muss dann folgenden Inhalt haben: #ct12345:SET:OUTPUT

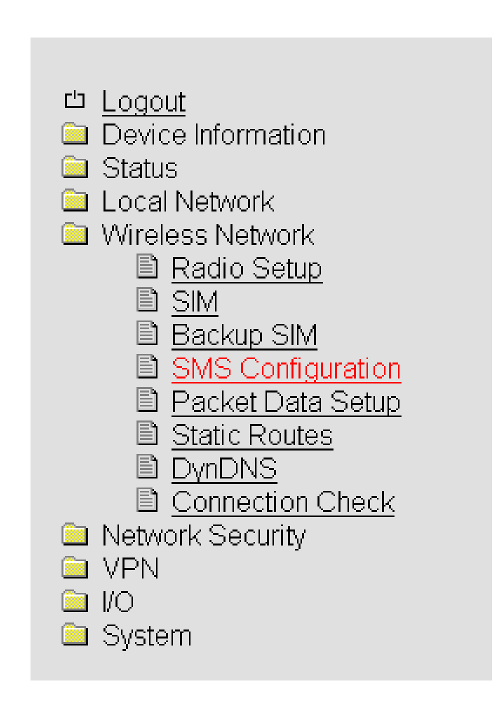
Weiterleitung einer SMS an einen Socket Server
Der Router kann empfangene SMS Nachrichten an ein Endgerät über die Ethernet Schnittstelle weiterleiten. Auf dem Endgerät muss dafür ein Socket Server zum Empfang von XML-Dateien installiert sein.
Klicken Sie Enable unter „SMS forward". Tragen Sie die Empfänger-IP-Adresse und den Port des Endgerätes ein, zu dem Sie kommunizieren möchten. Default-Wert für den Server ist Port 1432. Die empfangene SMS wird im folgenden Formatbeispiel weitergeleitet:

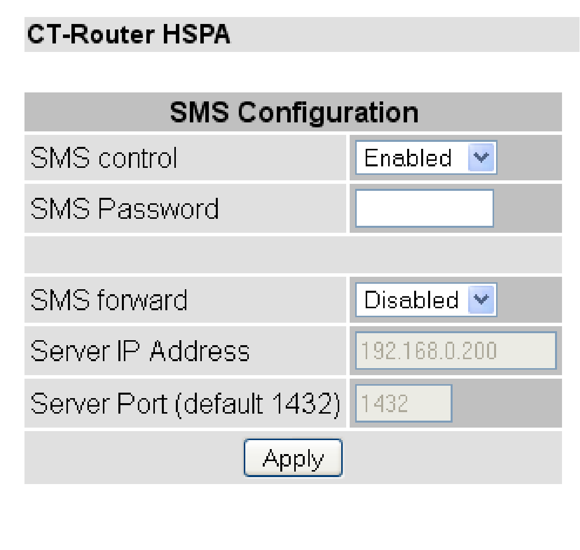
Wichtiger Hinweis!! Die Rufnummer muss dem Router zur Identifizierung als Eintragung im Telefonbuch bekannt sein.

Beispiel:
<?xml version="1.0"?>
<cmgr origaddr="+49172123456789" timestamp="10/05/21,11:27:14+08">
SMS message</cmgr>
origaddr = Rufnummer des Absenders
timestamp = Zeitstempel des Service Center im GSM 03.40 Format

Wireless Network

SMS Configuration

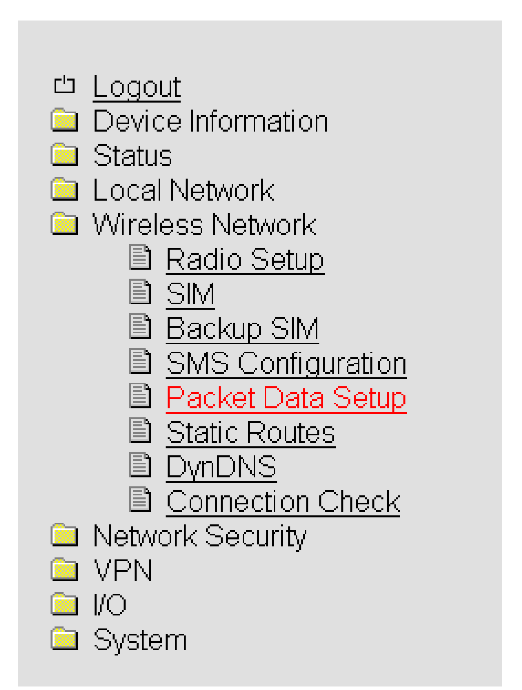


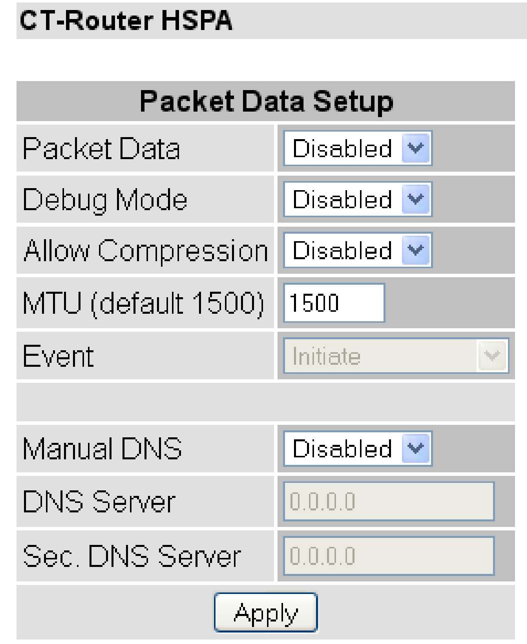


Wireless Network >> SMS Configuration	
SMS control	**Disable:** den Router per SMS steuern - deaktiviert **Enable:** den Router per SMS steuern - aktiviert
SMS Password	SMS-Passwort zum Steuern per SMS
SMS forward	**Disable:** SMS-Nachrichten über Ethernet weiterleiten - deaktiviert. **Enable:** SMS-Nachrichten über Ethernet weiterleiten - aktiviert.
Server IP Address	Weiterleitung der SMS erfolgt an diese IP-Adresse
Server Port (default 1432)	Weiterleitung der SMS erfolgt an diesen Port.

Wireless Network

Packet Data Setup

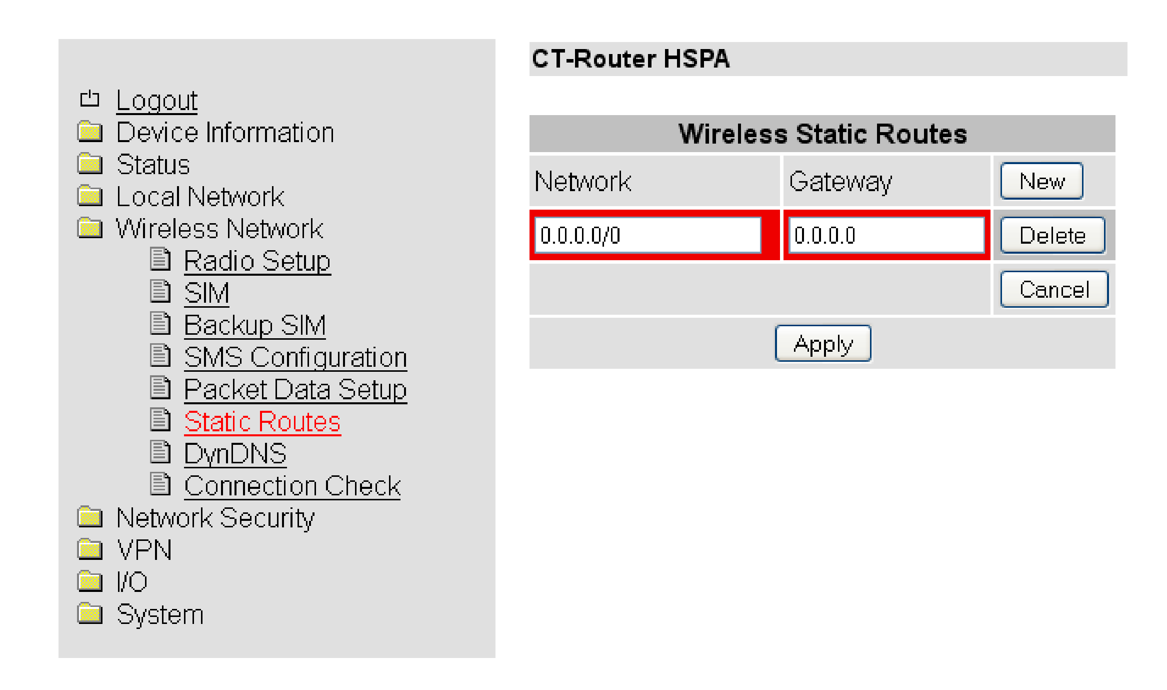




Wireless Network >> Packet Data Setup	
Packet Data	**Disable:** Deaktivierung der Paketdaten-Verbindung **Enable:** Aktivierung der Paketdaten-Verbindung / virtuelle dauerhafte Verbindung, erst bei tatsächlicher Datenübertragung entsteht Traffic.
Debug Mode	Zu Diagnosezwecken zur Paketdaten-Verbindung können Informationen im Log-File gespeichert werden. Diese Option kann aktiviert oder deaktiviert werden.
Allow Compression	**Disable:** Daten-Kompression aktiviert **Enable:** Daten Kompression deaktiviert
MTU (default 1500)	Maximale Paketgröße in Bytes
Event	**Initiate:** automatischer Start der Paketdaten-Verbindung **Initiate on Input #1... #4:** manueller Start über Schalteingang
Manual DNS	**Disable:** Deaktivierung der manuellen DNS-Einstellung (DNS wird vom Provider empfangen). **Enable:** Aktivierung der manuellen DNS-Einstellung
DNS Server	IP-Adresse, primärer DNS-Server im Mobilfunknetz
Sec. DNS Server	IP-Adresse, sekundärer DNS-Server im Mobilfunknetz

Wireless Network

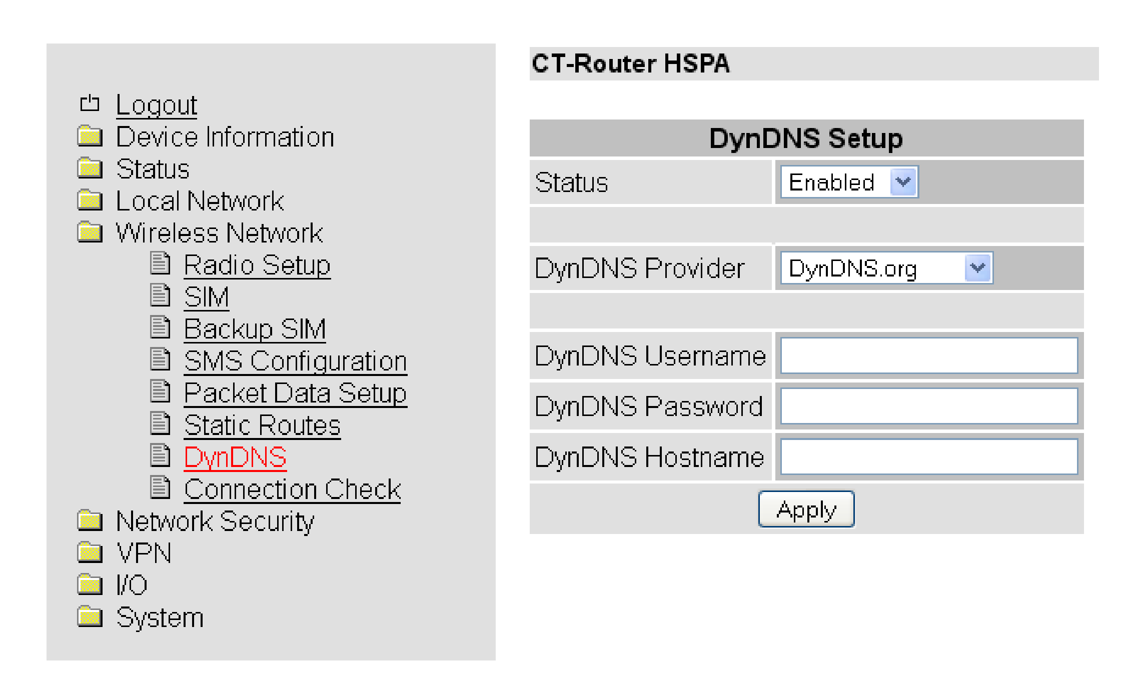
Static Routes



Wireless Network >> Static Routes	
Network	Netzwerk in CIDR-Form
Gateway	Gateway-Adresse des Netzwerkes
Max. 8 Netzwerke eintragbar	

Wireless Network

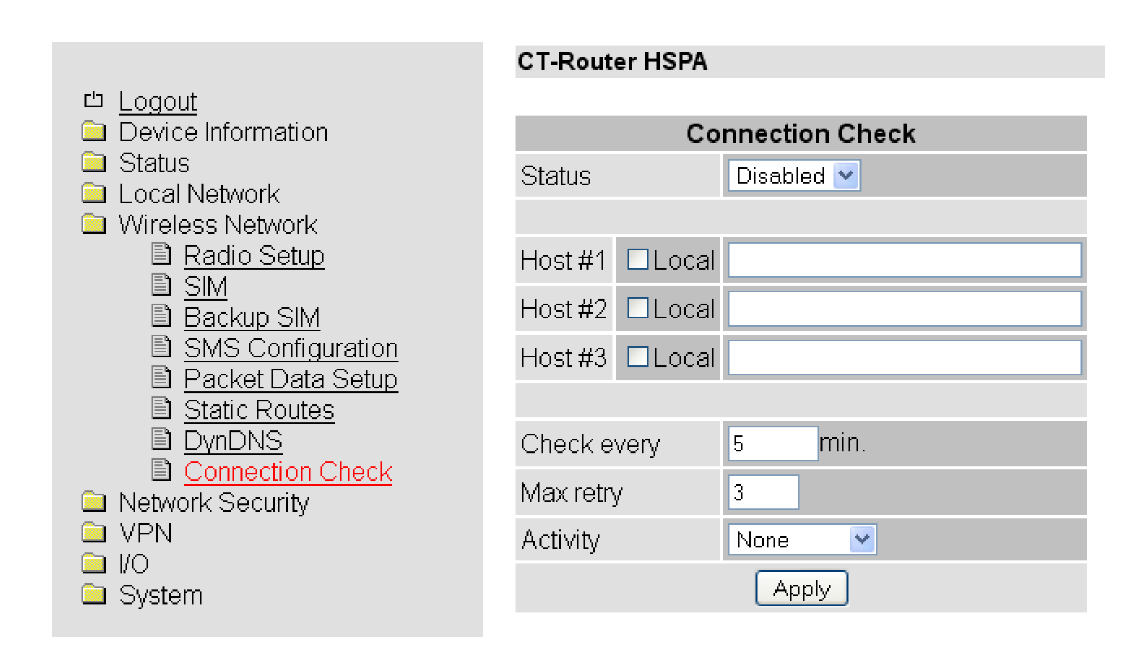
DynDNS



Wireless Network >> DynDNS	
DynDNS	**Disable:** Deaktivierung der DynDNS **Enable:** Aktivierung der DynDNS
DynDNS Provider	Auswahl des DynDNS-Anbieters
DynDNS Username	Benutzername des DynDNS-Accounts
DynDNS Password	Passwort des DynDNS-Accounts
DynDNS Hostname	Hostname des Routers beim DynDNS-Service

Wireless Network

Connection Check

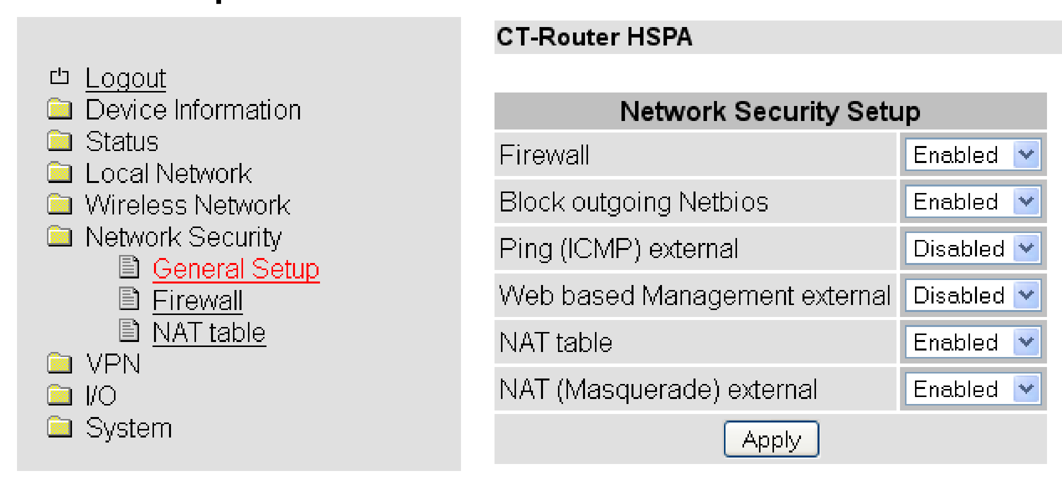


Wireless Network >> Connection Check	
Connection Check	**Disable:** Deaktivierung der Verbindungsprüfung der Paketdaten-Verbindung **Enable:** Aktivierung der Verbindungsprüfung der Paketdaten-Verbindung
Host #1…#3	IP-Adresse oder Hostnamen als Referenzpunkt zur Verbindungsprüfung **Local:** Aktivierung bei Adressen, die über einen VPN-Tunnel erreichbar sind
Check every	Es wird alle x Minuten die Verbindung geprüft.
Max. retry	Maximale Anzahl der Verbindungsversuche
Activity	Bei Verbindungsabbruch eine der folgenden Aktionen ausführen: **Reboot:** Router Neustart **Reconnect:** Verbindung wird versucht neu aufzubauen **Relogin:** Mobilfunkinterface wird heruntergefahren und erneuter Versuch eines Verbindungsaufbaus mit Login. **None:** keine Aktion wird ausgeführt

Network Security

In diesem „Network Security"-Menü nehmen Sie Einstellungen zu Netzwerksicherheit vor.

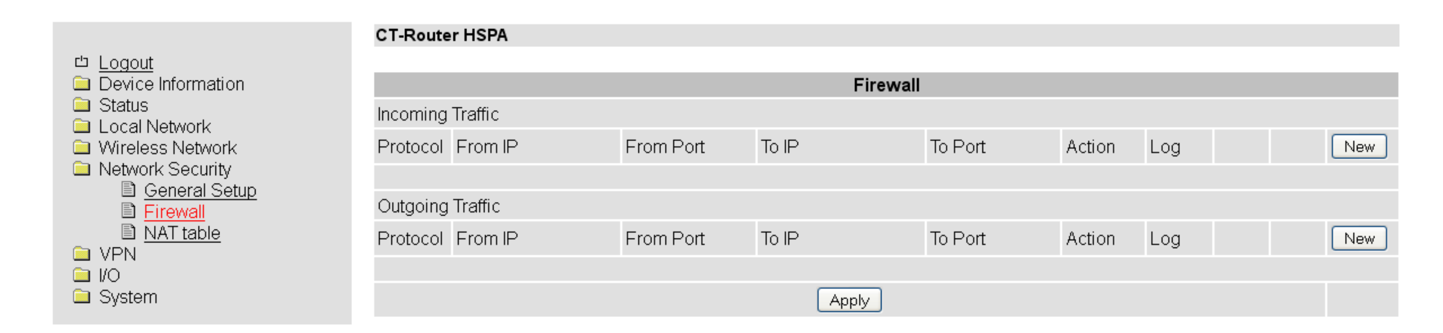
General Setup



Network Security >> General Setup	
Firewall	**Disable:** Deaktivierung der integrierten Stateful Packet Inspection Firewall **Enable:** Aktivierung der integrierten Stateful Packet Inspection Firewall
Block outgoing Netbios	Netbios-Anfragen gehen von Windows-Systemen im lokalen Netzwerk aus und verursachen einen erhöhten Datenverkehr. **Disable:** Netbios-Anfragen werden erlaubt **Enable:** Netbios-Anfragen werden geblockt
Ping (ICMP) external	Ping-Anfragen prüfen, ob ein Gerät im Netzwerk erreichbar ist. Dadurch erhöht sich der Datenverkehr. **Disable:** Ping-Anfragen aus dem externen IP-Netz werden nicht beantwortet **Enable:** Ping-Anfragen aus dem externen IP-Netz werden beantwortet
Web based Management external	**Disable:** Externe WBM Konfiguration ist deaktiviert **Enable:** Externe WBM Konfiguration ist aktiviert
NAT (Masquerade) external	**Disable:** IP-Masquerading deaktiviert **Enable:** IP-Masquerading aktiviert

Network Security

Firewall

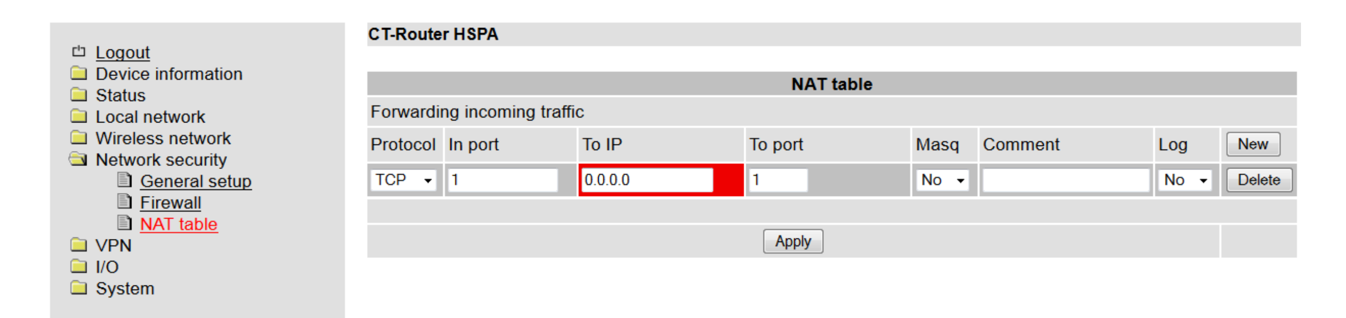


Network Security >> Firewall	
Incoming Traffic	
Protocol	Protokollauswahl: TCP, UDP, ICMP, all
From IP / To IP	IP-Adressenbereich in CIDR-Form (0.0.0.0/0 bedeutet alle IP-Adressen)
From Port / To Port	Portbereich ("any" bezeichnet alle Ports)
Action	**Accept:** Datenpakete werden angenommen. **Reject:** Datenpakete werden abgelehnt. Benachrichtigung an den Absender, dass die Daten abgelehnt werden. **Drop:** Datenpakete werden "fallen gelassen" d.h. sie werden abgewiesen und der Absender erhält keine Benachrichtigung.
Log	**Yes:** Aktivierung der Regel wird protokolliert **No:** Aktivierung der Regel wird nicht protokollier.
New / Delete	Neue Regel aufstellen / bestehende Regel löschen
	Mit den Pfeilen können Regeln nach oben oder unten verschoben werden.
Outgoing Traffic	Verhält sich ähnlich zum „Incoming Traffic“, jedoch beziehen sich diese Regeln auf den ausgehenden Datenverkehr. Ist keine Regel vorhanden, so sind alle ausgehenden Verbindungen verboten (mit Ausnahme von VPN-Verbindungen)

Network Security

NAT Table

Der Router hat nur eine IP-Adresse, über die von außen auf ihn zugegriffen werden kann.
Über zusätzlich übermittelte Portnummern können Datenpakete auf Ports interner IP-Adressen umgeleitet werden.



Network Security >> NAT Table	
Protocol	Protokollauswahl: TCP, UDP, ICMP, all
In Port	bei TCP und UDP haben Sie folgende Optionen: direkte Port-Angabe z.B: In Port = 20, Portbereiche z.B: In Port = 20-30
To Port	To Port= ersten Port eintragen
To IP	Ziel IP-Adresse (0.0.0.0 bedeutet ungültig)
Masq (IP-Masquerading)	**Die interne IP-Adresse wird ersetzt durch die IP-Adresse des Routers (ausgehend Daten Paketen) und umgekehrt bei eingehenden Daten Paketen.** **Yes:** IP-Masquerading aktiviert **No:** IP-Masquerading deaktiviert
Log	**Yes:** Aktivierung der Regel wird protokolliert **No:** Aktivierung der Regel wird nicht protokolliert
New / Delete	Neue Regel aufstellen / bestehende Regel löschen
	Mit den Pfeilen können Regeln nach oben oder unten verschoben werden.

VPN

Im Menü VPN können Sie einerseits Einstellungen zur Internet Protocol Security (IPsec) andererseits zum virtuellen privaten Netzwerk (OpenVPN) vornehmen.

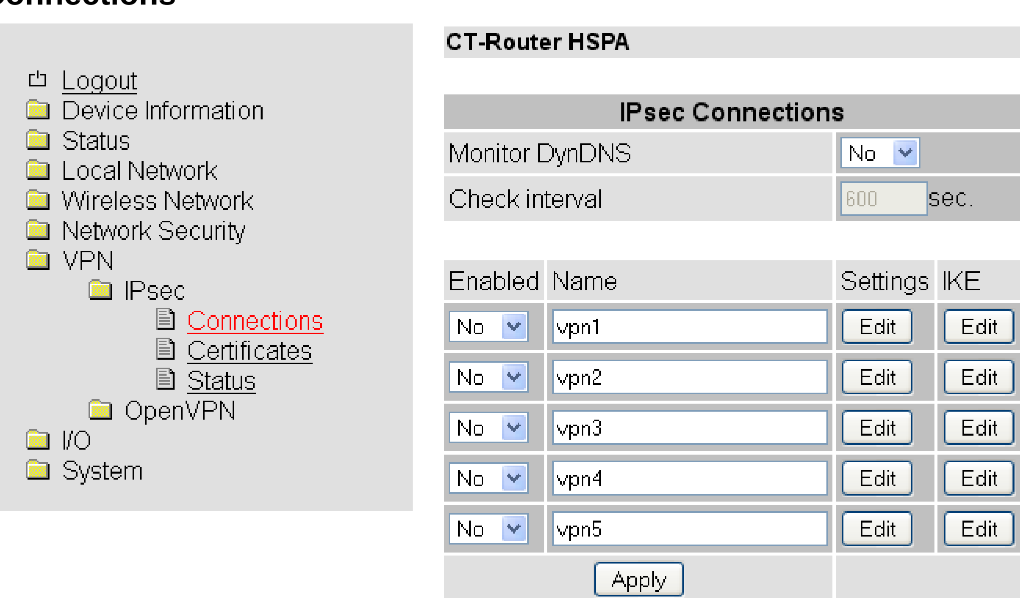
Für eine VPN-Verbindung müssen die IP-Adressen der VPN-Gegenstellen bekannt und adressierbar sein.

IPSec

Die VPN-Gegenstelle muss IPsec mit folgender Konfiguration unterstützen:

- Authentifizierung über X.509-Zertifikate oder Preshared Secret Key (PSK)
- ESP
- Diffie-Hellman Gruppe 2 oder 5
- 3DES oder AES encryption
- MD5 oder SHA-1 Hash Algorithmen
- Tunnel-Modus
- Quick Mode
- Main Mode
- SA Lifetime (1 Sekunde bis 24 Stunden)

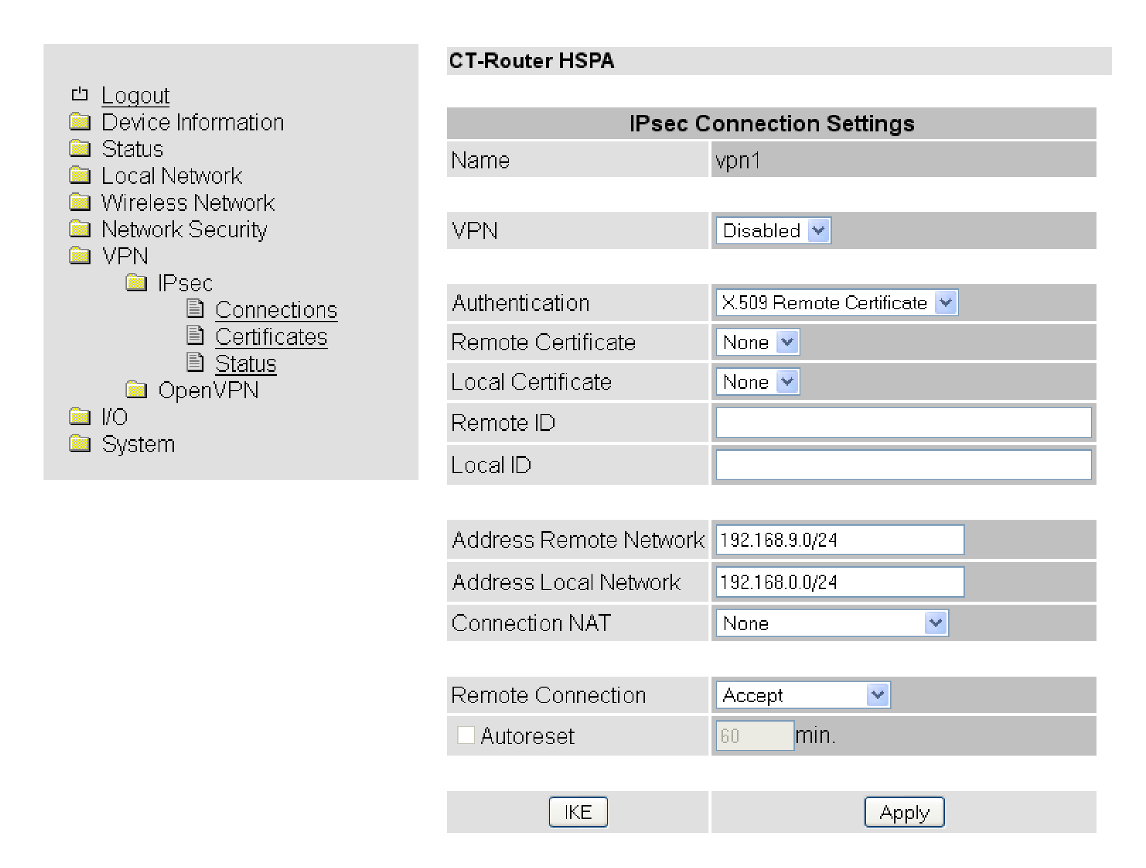
Connections



VPN >> IPsec >> Connections	
Monitor DynDNS	VPN-Gegenstelle hat keine feste IP und als Remote Host wird ein DynDNS-Name genutzt, so kann diese Funktion aktiviert werden, um die Verbindung zu überprüfen.
Check Interval	Prüfintervall in Sekunden
Enable	VPN-Verbindung aktivieren (=Yes) oder deaktivieren (=No)
Name	Name der VPN-Verbindung festlegen
Settings	Einstellungen für IPsec
IKE	Einstellungen für das Internet-Key-Exchange-Protokoll

VPN-IPsec

Connections Settings



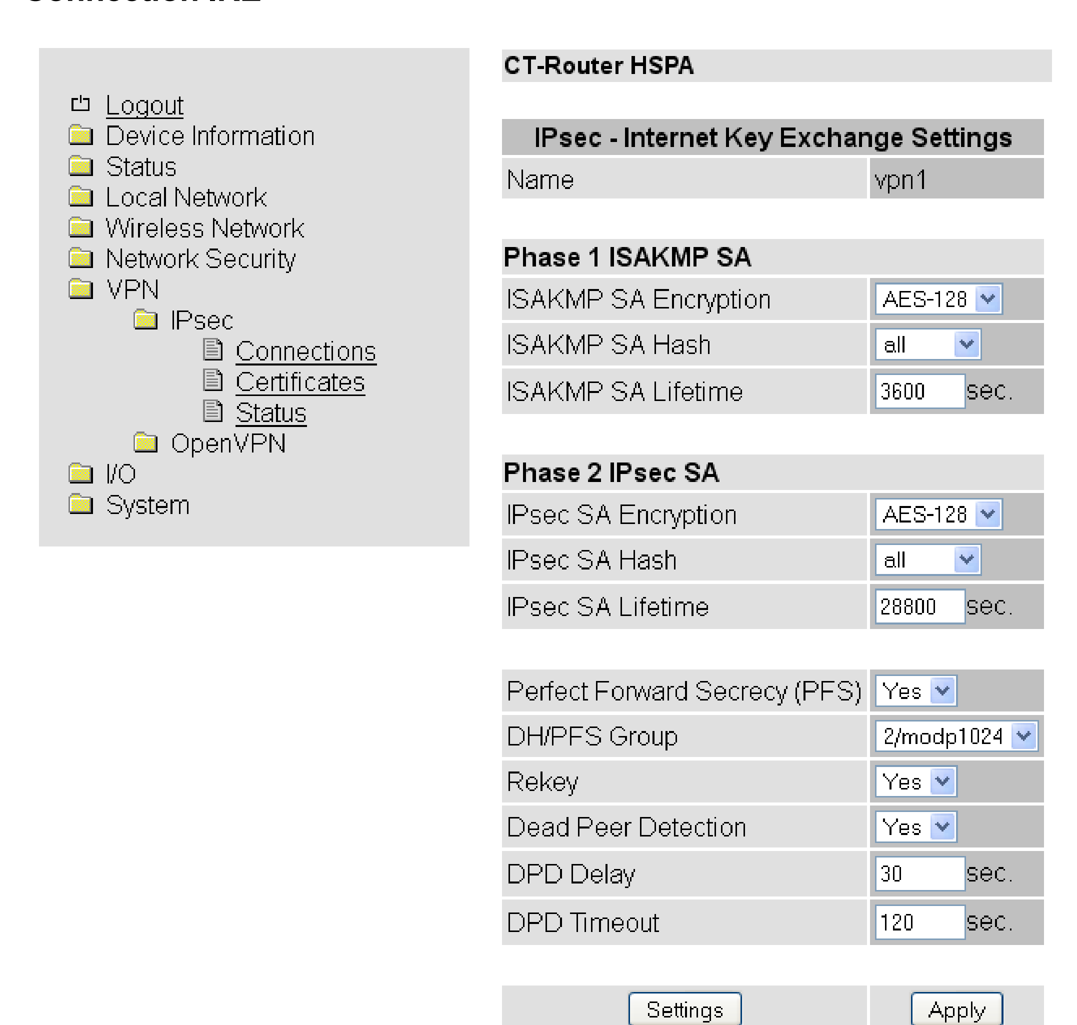
VPN >> IPsec >> Connections >> Settings >> Edit	
Name	Name der VPN-Verbindung
VPN	Aktivieren (=Enable) oder Deaktivieren (=Disable) der VPN-Verbindung
Remote Host	IP-Adresse / URL der Gegenstelle Kann nur eingestellt werden, wenn unter Remote Connection "Initiate" ausgewählt wurde. Wurde unter Remote Connection "Accept" ausgewählt, so wird der Wert für Remote Host auf "%any" gesetzt, und es wird auf eine Verbindung gewartet.
Authentication	X.509 Remote Certificate - VPN-Teilnehmer haben einen privaten und einen öffentlichen Schlüssel (X.509-Zertifikat). Preshared Secret Key - VPN-Teilnehmer besitzen einen privaten Schlüssel (ein gemeinsames Passwort).
Remote Certificate	VPN-Gegenstellen Authentifizierung erfolgt über ein Zertifikat, das in dem Menü "IPsec Certificates" hochgeladen werden muss.
Local Certificate	Router Authentifizierung bei der VPN-Gegenstelle erfolgt über ein Zertifikat, das in dem Menü "IPsec Certificates" hochgeladen werden muss.

VPN-IPsec

Remote ID	**Leer:** Kein Eintrag in der Zeile bedeutet, dass die Angaben aus dem Zertifikat gewählt werden. **Subject:** Eine IP-Adresse, E-Mail-Adresse oder ein Hostname bedeutet, dass diese Einträge auch im Zertifikat vorhanden sein sollten, damit sich der Router authentifizieren kann.
Local ID	Siehe Remote ID
Address Remote Network	IP-Adresse/Subnetzmaske des Netzwerkes, zu dem eine VPN-Verbindung aufgebaut wird.
Address Local Network	IP-Adresse/Subnetzmaske vom lokalen Netzwerk.
Local 1:1 NAT	IP-Adresse vom lokalen Netzwerk, unter der das Netzwerk per 1:1 NAT aus dem Remote-Netz erreicht werden kann/soll.
Remote Connection	**Accept:** VPN-Verbindung wird von einer Gegenstelle aufgebaut und vom Router akzeptiert. **Initiate:** VPN-Verbindung geht vom Router aus. **Initiate on Input:** Startet / Stoppt den VPN-Tunnel durch digitalen Eingang. **Initiate on SMS:** VPN-Verbindung wird durch eine SMS gestartet **Initiate on Call:** VPN-Verbindung wird durch einen Anruf gestartet
Autoreset	Kann bei "Initiate on SMS" und muss bei "Initiate on Call" festgelegt werden. Es wird ein Zeitraum festgelegt, nach wieviel Minuten die VPN-Verbindung per Autoreset gestoppt wird.

VPN-IPsec

Connection IKE



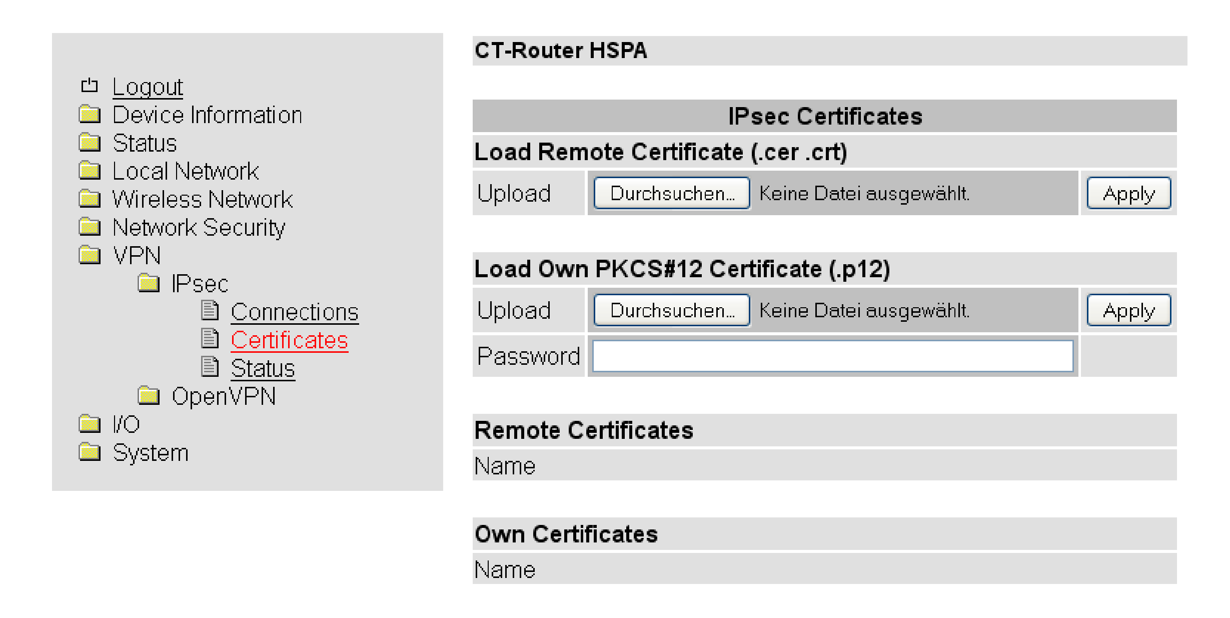
VPN >> IPsec >> Connections >> IKE >> Edit	
Name	Name der VPN-Verbindung.
Phase 1 ISAKMP SA	Schlüsselaustausch
ISAKMP SA Encryption	Verschlüsselungsalgorithmus-Auswahl
ISAKMP SA Hash	Hash-Algorithmus-Auswahl
ISAKMP SA Lifetime	Lebensdauer des ISAKMP SA Schlüssels. Standardeinstellung 3600 Sekunden (1 Stunde) max. Einstellwert 86400 Sekunden (24 Stunden)
Phase 2 IPsec SA	Datenaustausch
Ipsec SA Encryption	siehe ISAKMP SA Encryption
Ipsec SA Hash	siehe ISAKMP SA Hash
Ipsec Lifetime	Lebensdauer des Ipsec SA Schlüssels. Standardeinstellung 28800 Sekunden (8 Stunden) max. Einstellwert 86400 Sekunden (24 Stunden)

VPN-IPsec

Perfect Forward Secrecy (PFS)	Aktivieren (=Yes) oder Deaktivieren (=No) der PFS Funktion.
DH/PFS Group	Im Ipsec werden beim Datenaustausch in bestimmten Intervallen die Schlüssel erneuert. Mit PFS werden hierbei mit der Gegenstelle im Schlüsselaustauschverfahren neue Zufallszahlen ausgehandelt. Auswahl des Verfahrens.
Dead Peer Detection	Unterstützt die Gegenstelle ein solches Protokoll, so kann überprüft werden, ob die Verbindung "tot" ist oder nicht. Die Verbindung wird versucht neu aufzubauen. **No:** Keine Dead Peer Detection **Yes:** Bei VPN Initiate wird versucht, neuzustarten "Restart. Bei VPN Accept wird die Verbindung geschlossen "Clear".
DPD Delay (sec.)	Zeitintervall in Sekunden, in dem die Peer-Verbindung überprüft wird.
DPD Timeout (sec.)	Zeitspanne in Sekunden nach der ein Timeout erfolgen soll.

VPN-IPsec

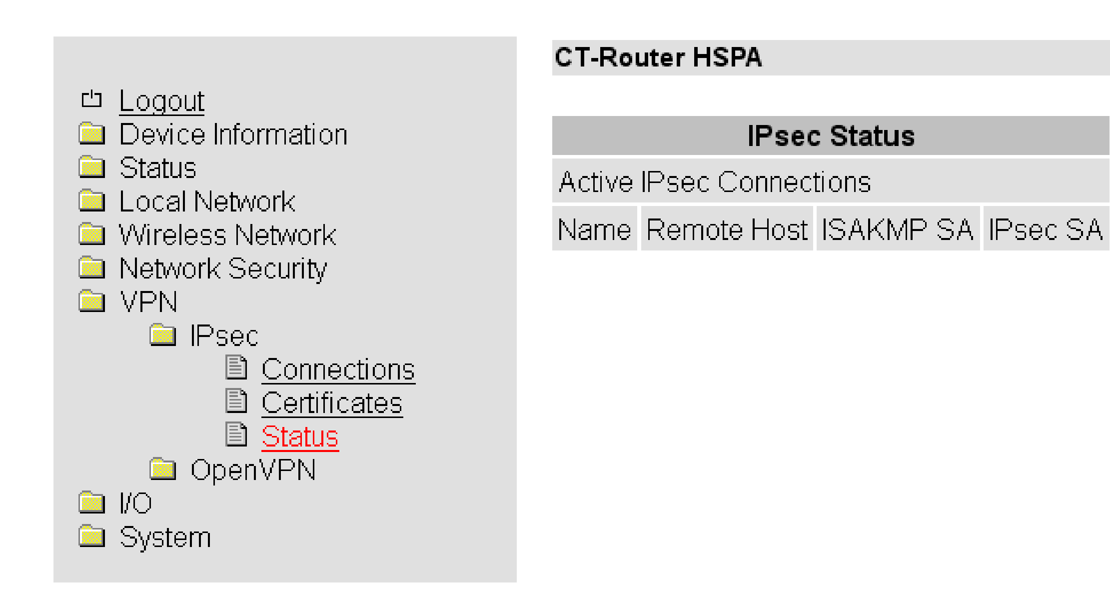
Certificates



VPN >> IPsec >> Certificates	
Load Remote Certificate	Hochladen von Zertifikaten, mit denen eine Authentifizierung für den Router bei der VPN-Gegenstelle erfolgen kann.
Load Own PKCS#12 Certificate	Hochladen eines Zertifikats (Providervorgabe)
Password	Passwort für das PKCS#12 Zertifikat / das Passwort wird beim Export vergeben
Remote Certificates	Tabellarische Übersicht aller "Remote Certificates" / mit "Delete" wird ein Zertifikat gelöscht
Own Certificates	Tabellarische Übersicht aller "Own Certificates" / mit "Delete" wird ein Zertifikate gelöscht

VPN-IPsec

Status

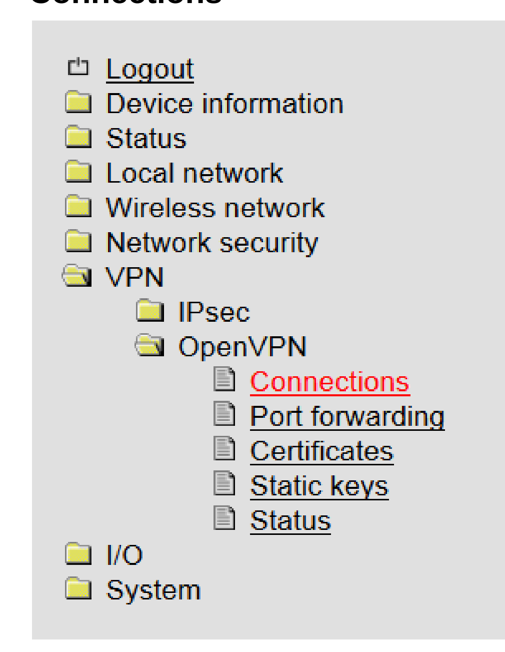


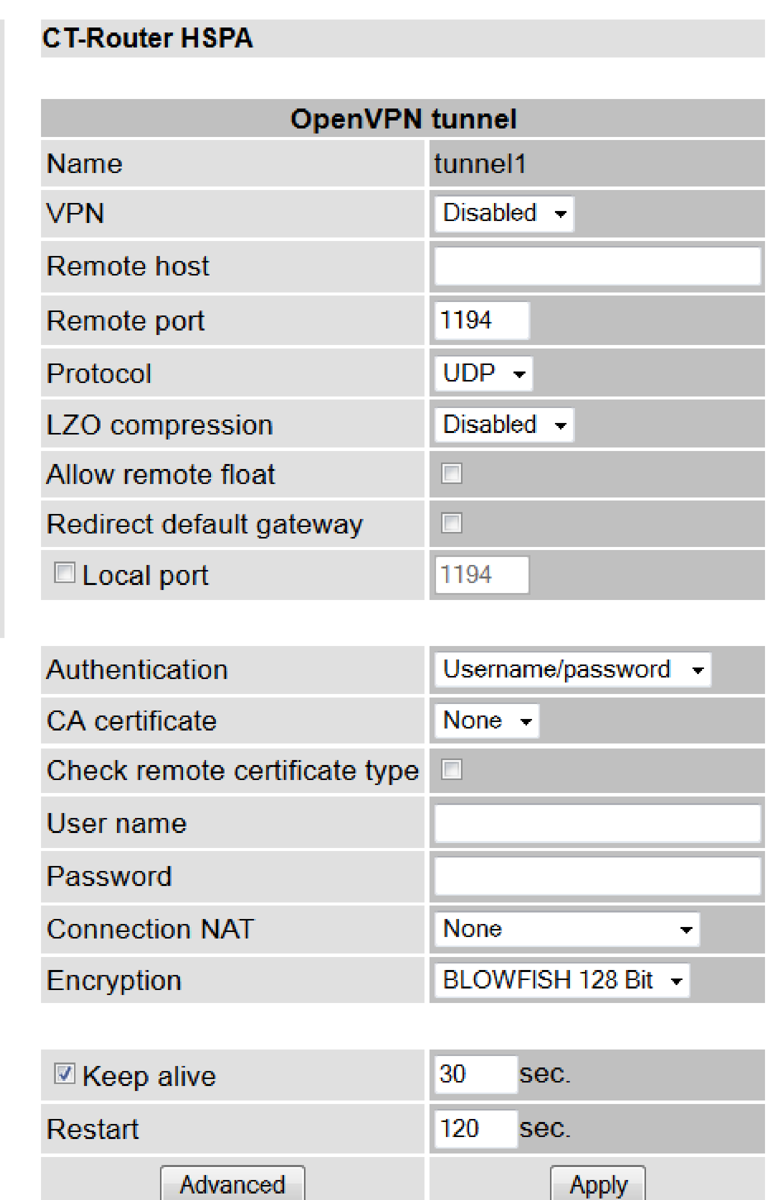
VPN >> IPsec >> Status	
Name	Name der VPN-Verbindung
Remote Host	IP-Adresse oder URL der Gegenstelle
ISAKMP SA	Aktiv (grünes Feld)
IPSec SA	Aktiv (grünes Feld)

VPN - OpenVPN

OpenVPN

Connections





VPN >> OpenVPN >> Connections	
VPN	OpenVPN Tunnel aktiv (=Enable) oder inaktiv (=Disable)
Name	Name der OpenVPN-Verbindung
Remote Host	IP-Adresse oder URL der Gegenstelle
Remote Port	Port der Gegenstelle (Standard: 1194)
Protocol	UDP- oder TCP-Protokoll für die OpenVPN-Verbindung festlegen!
LZO Compression	**Disabled:** Keine Kompression **Adaptive:** Adaptive Kompression **Yes:** Kompression aktiviert

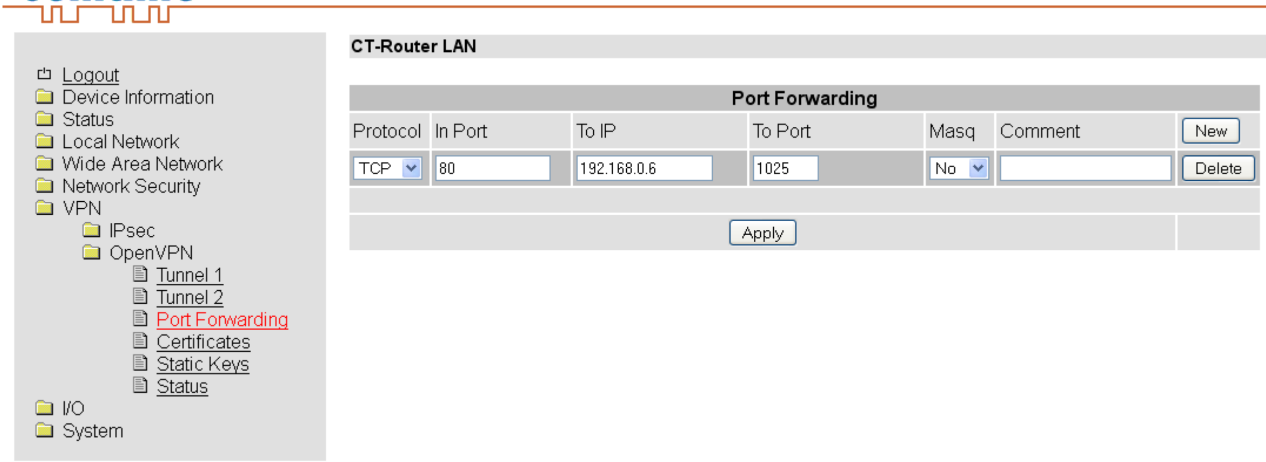
VPN - OpenVPN

Allow Remote Float	Option: Bei der Kommunikation mit dynamischen IP-Adressen akzeptiert die OpenVPN-Verbindung authentifizierte Pakte von jeder IP-Adresse.
Local Port	Lokaler Port
Authentication	Authentifizierungsart der OpenVPN-Verbindung festlegen (X.509, PSK oder Username/Password)!
Local Certifacation	Zertifikat vom Router für die Authentifizierung bei der Gegenstelle
Check Remote Certificate Type	Option: Zertifikate der OpenVPN-Verbindung überprüfen
Address Local Network	IP-Adresse/Subnetzmaske des lokalen Netzwerks
Local 1:1 NAT	Option: IP-Adresse vom lokalen Netzwerk, unter der das Netzwerk per 1:1 NAT aus dem Remote-Netz erreicht werden kann/soll.
Encryption	Verschlüsselungsalgorithmus der OpenVPN-Verbindung
Keep Alive	Zeitintervall in Sekunden von Keep Alive-Anfragen an die Gegenstelle
Restart	Zeitspanne in Sekunden nach der die Verbindung neu gestartet werden soll, falls keine Antwort auf die Keep Alive-Anfragen erfolgt.

VPN - OpenVPN

Port Forwarding

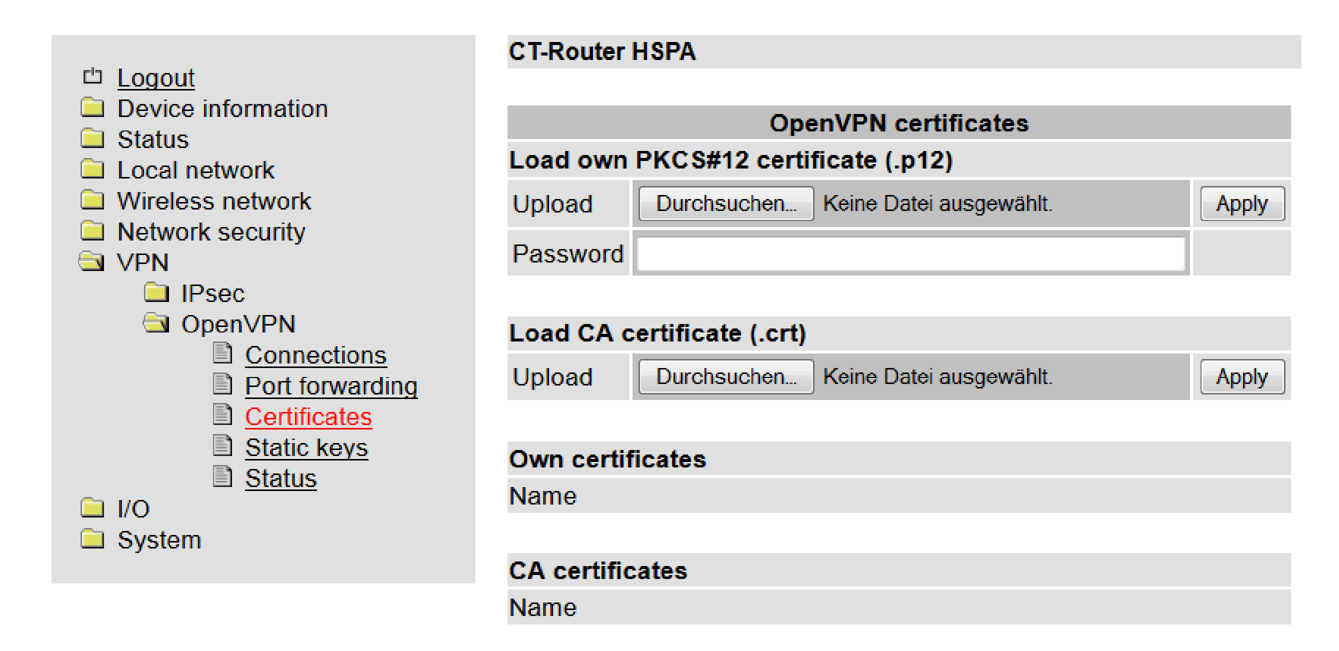




VPN >> OpenVPN >> Port Forwarding	
Protocol	Auswahl: TCP / UDP / ICMP
In Port	Port Nr. eingehende Verbindung
To IP	IP Adresse von Ziel
To Port	Port Nr. Vom Ziel

VPN - OpenVPN

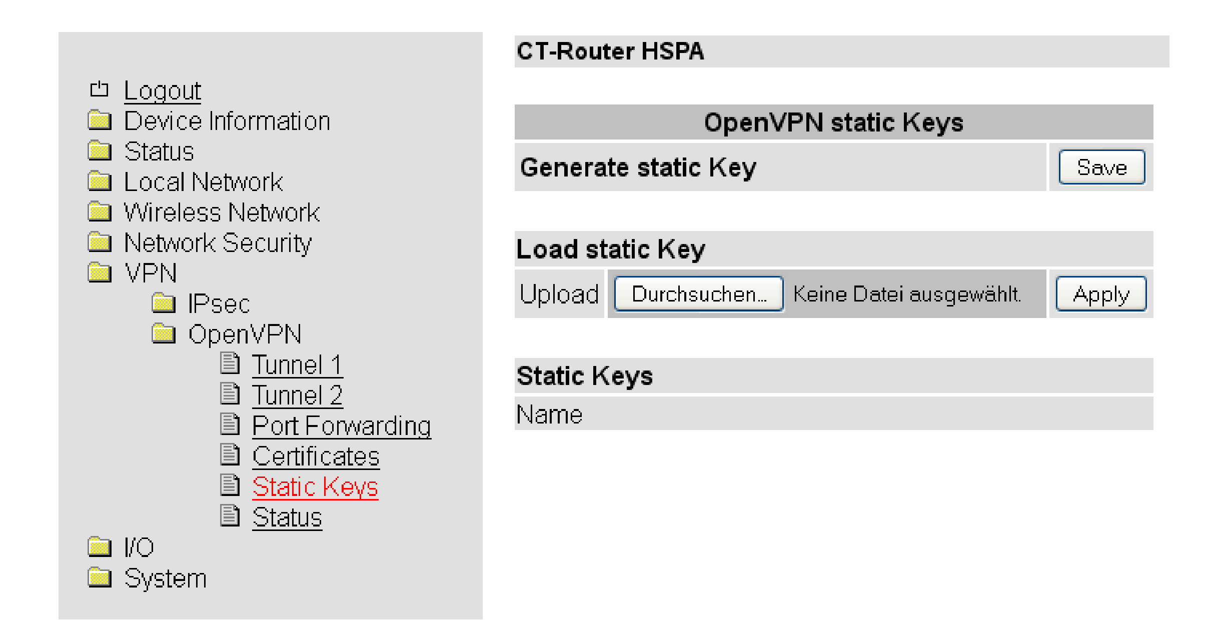
Certificates



VPN >> OpenVPN >> Certificates	
Load Own PKCS#12 Certificate	Hochladen eines Zertifikats, das von Ihrem Provider stammt.
Password	Passwort für das PKCS#12 Zertifikat. Das Passwort wird beim Export vergeben.
Own Certificates	Tabellarische Übersicht aller "Own Certificates" / mit "Delete" werden die Zertifikate gelöscht

VPN - OpenVPN

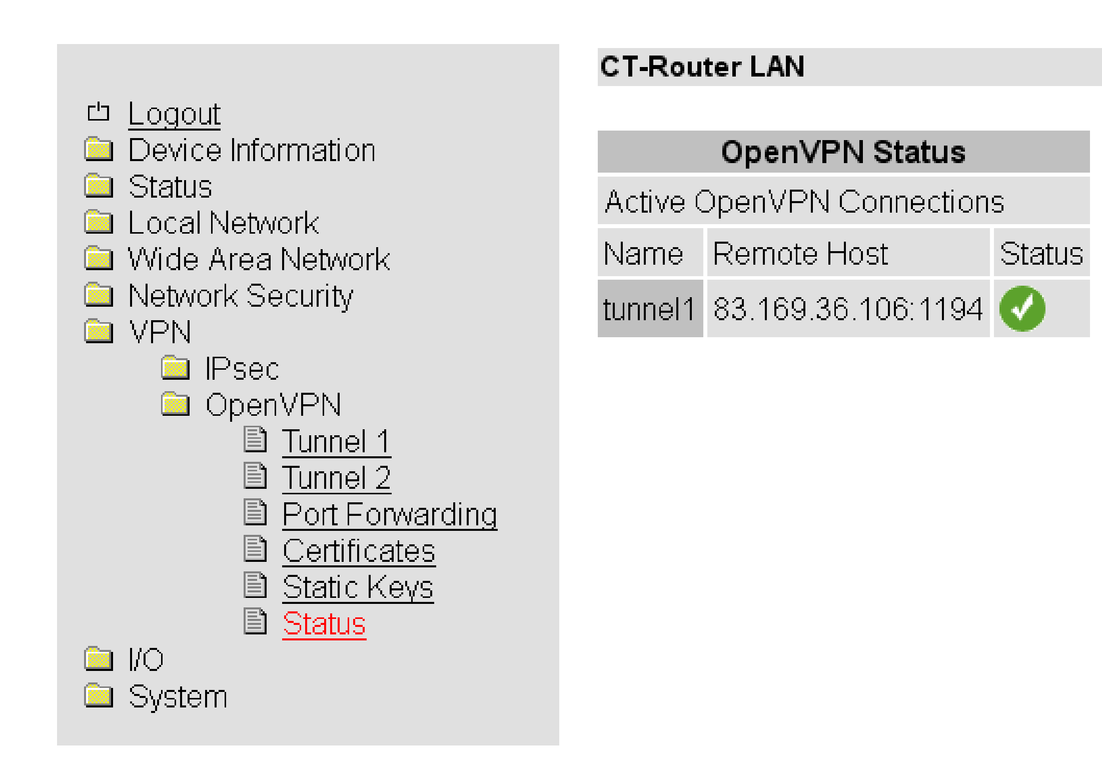
Static Keys



VPN >> OpenVPN >> Static Keys	
Generate static Key	Einen statischen Schlüssel generieren und speichern.
Load static Key	Statischen Schlüssel in den Router laden (den gleichen statischen Schlüssel muss auch die Gegenstelle besitzen).
Static Keys	Tabellarische Übersicht aller geladenen statischen Schlüssel.

VPN - OpenVPN

Status

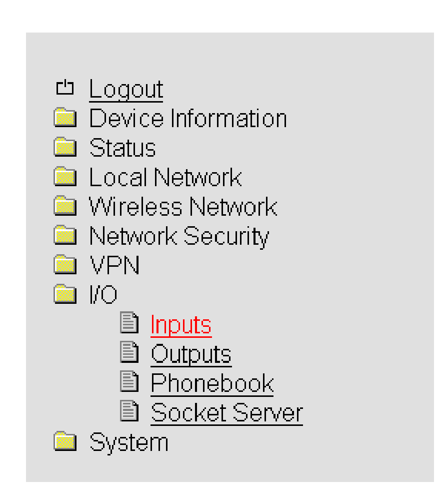


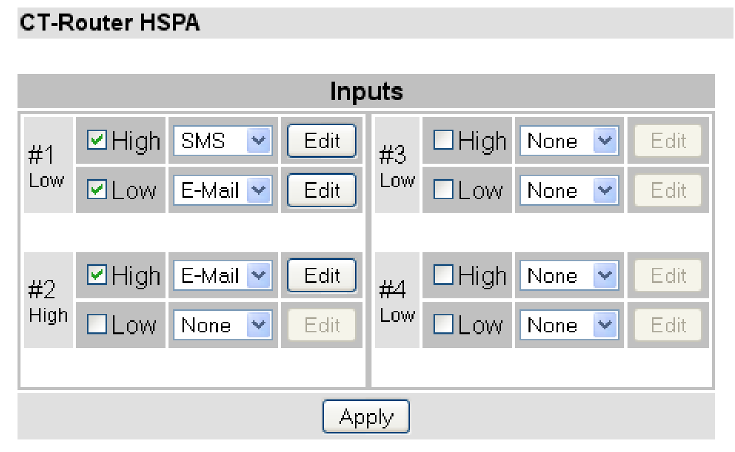
VPN >> OpenVPN >> Status	
Name	Name der VPN-Verbindung
Remote Host	IP-Adresse oder URL der Gegenstelle
Status	Aktiv (=grünes Feld)

I/O

Der CT-Router HSPA verfügt über vier digitale Ein- und Ausgänge, die in dem „I/O"-Menü von Ihnen konfiguriert werden können.

Inputs





I/O >>Inputs	
High	Option: Bei einem High-Pegel kann eine Nachricht per SMS oder E-Mail verschickt werden.
Low	Option: Bei einem Low-Pegel kann eine Nachricht per SMS oder E-Mail verschickt werden.
Stellt man nun eine der oben dargestellten Optionen ein, so muss man diese mit "apply" bestätigen. Erst dann können die Einstellungen für die Benachrichtigung editiert werden. SMS: Eine oder mehrere Rufnummern werden aus dem eingespeicherten Telefonbuch selektiert, und Sie können einen individuellen Nachrichtentext festlegen. E-Mail: Sie können einen Empfänger, einen Kopie-Empfänger, einen Betreff und einen Nachrichtentext festlegen.	

Schalteingänge anschließen

- Schließen Sie die Schalteingänge an den jeweiligen steckbaren Schraubklemmen an.
- An die Schalteingänge (I1 ... I4) können Sie 10 ... 30 V DC anschließen.
- Das 0-V-Potential der Schalteingänge müssen Sie an die "0 V" Klemme des Spannungs-Anschlusses anschließen.

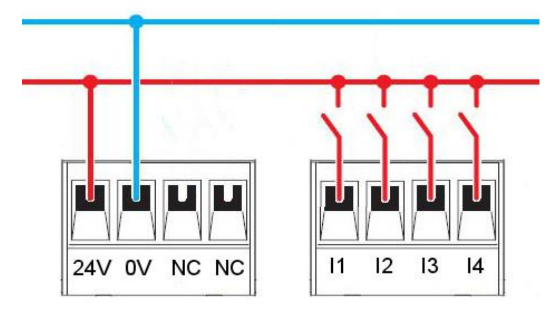
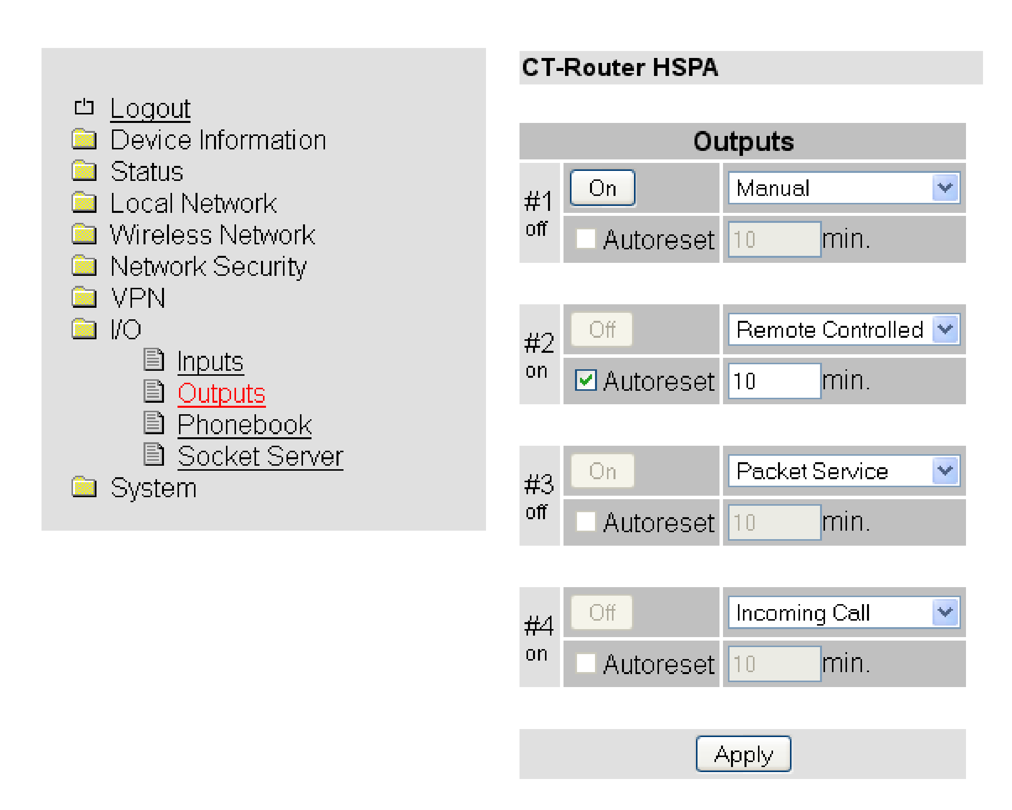
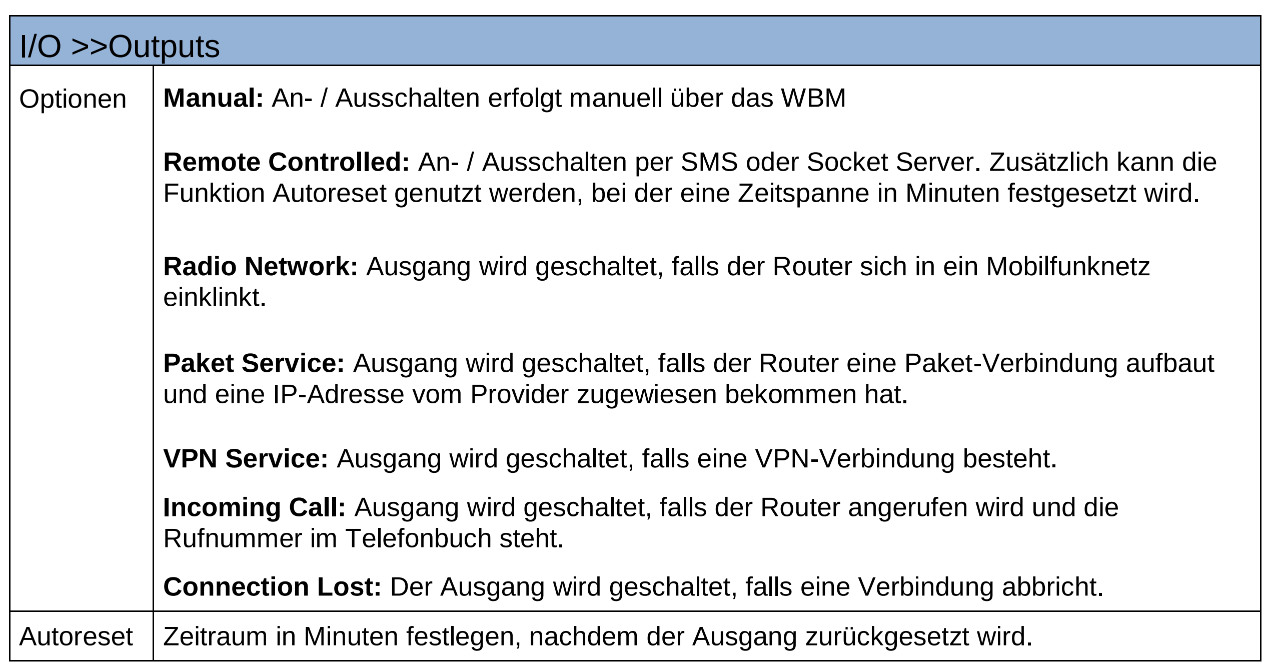


Bild Verdrahtung der Eingänge

I/O

Outputs





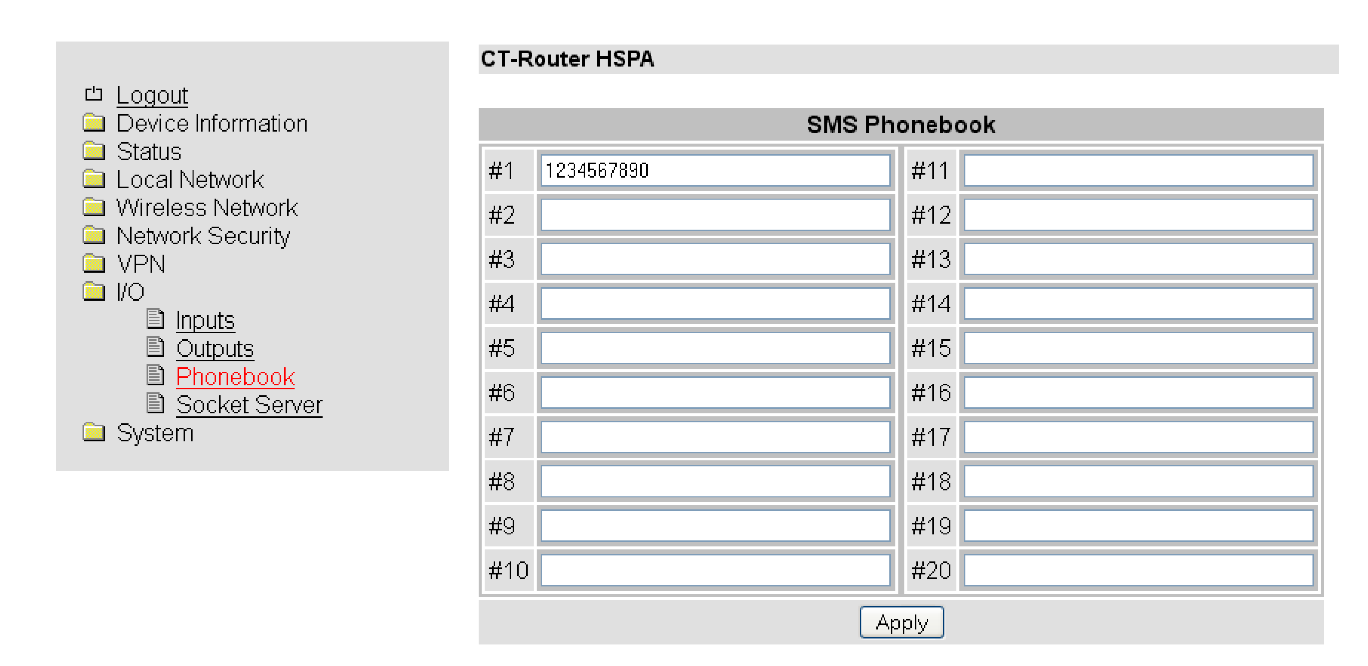
I/O >>Outputs	
Optionen	**Manual:** An- / Ausschalten erfolgt manuell über das WBM **Remote Controlled:** An- / Ausschalten per SMS oder Socket Server. Zusätzlich kann die Funktion Autoreset genutzt werden, bei der eine Zeitspanne in Minuten festgesetzt wird. **Radio Network:** Ausgang wird geschaltet, falls der Router sich in ein Mobilfunknetz einklinkt. **Paket Service:** Ausgang wird geschaltet, falls der Router eine Paket-Verbindung aufbaut und eine IP-Adresse vom Provider zugewiesen bekommen hat. **VPN Service:** Ausgang wird geschaltet, falls eine VPN-Verbindung besteht. **Incoming Call:** Ausgang wird geschaltet, falls der Router angerufen wird und die Rufnummer im Telefonbuch steht. **Connection Lost:** Der Ausgang wird geschaltet, falls eine Verbindung abbricht.
Autoreset	Zeitraum in Minuten festlegen, nachdem der Ausgang zurückgesetzt wird.

Die kurzschlussfesten Schaltausgänge (O1 ... O4) sind für maximal 150 mA bei 10 ... 30 V DC ausgelegt.

Das 0-V-Potential der Schaltausgänge müssen Sie an die "0 V" Klemme des Spg-Anschlusses anschließen

I/O

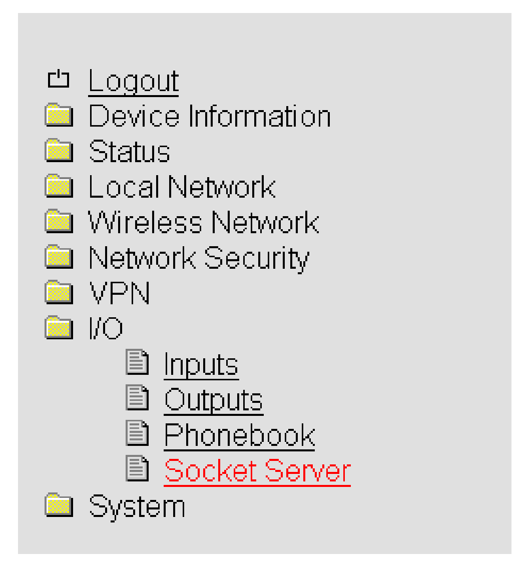
Phonebook

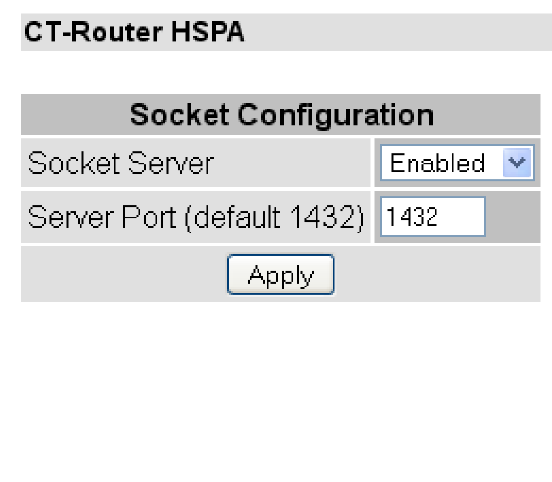


I/O >> Phonebook	
#1 … #20	Rufnummern für I/O Input und I/O Output

I/O

Socket Server



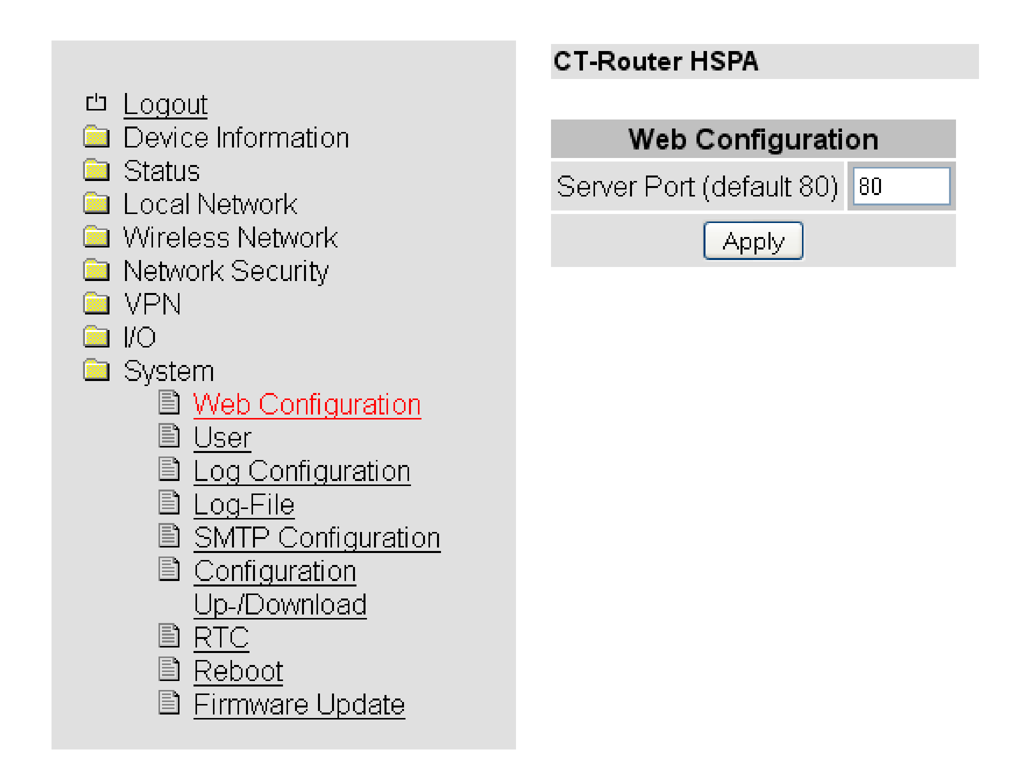


I/O >> Socket Server	
Socket Server	**Disable:** Ansteuern des Routers über Ethernet deaktiviert **Enable:** Ansteuern des Routers über Ethernet aktiviert
Server Port (default 1432)	Socket Server Port festlegen (Port 80 kann nicht genutzt werden). Daten, die an den Router geschickt werden, müssen XML Version 1.0 konform sein. Beispiel: <?xml version="1.0"?> <io> <input no="1" value="on"> <output no="2" value="off"> <output no="3" /> </io>

System

Im Systemmenü können allgemeine Einstellungen für den CT-Router HSPA getroffen werden.

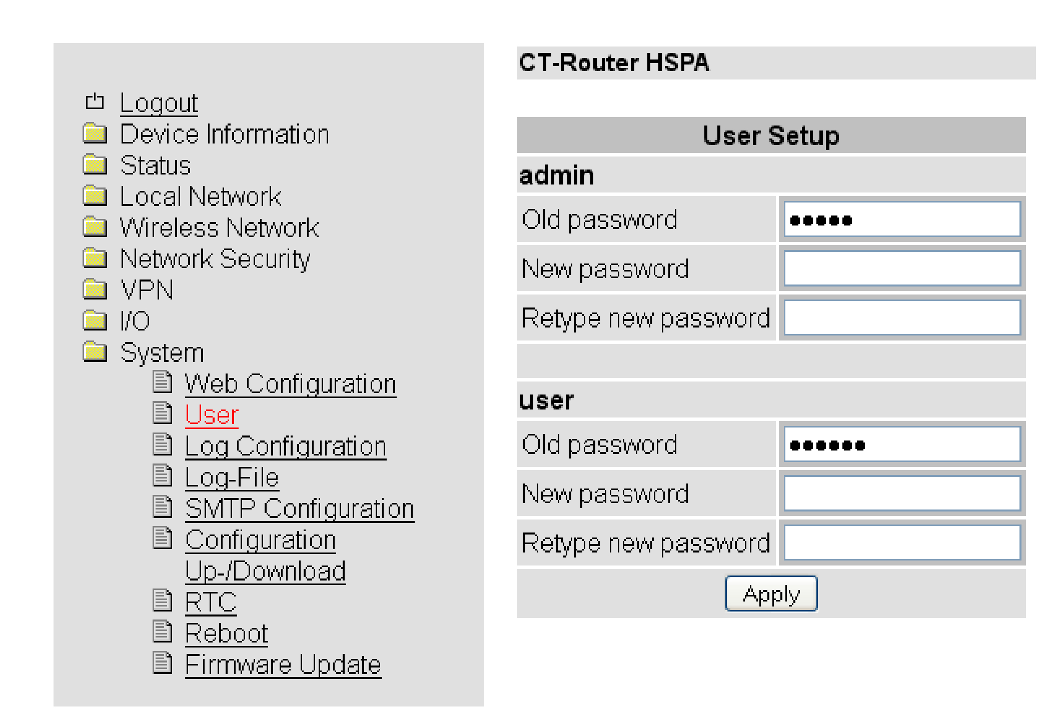
Web Configuration



System >> Web Configuration	
Server Port (default 80)	Porteinstellung für WBM über Internetbrowser.

System

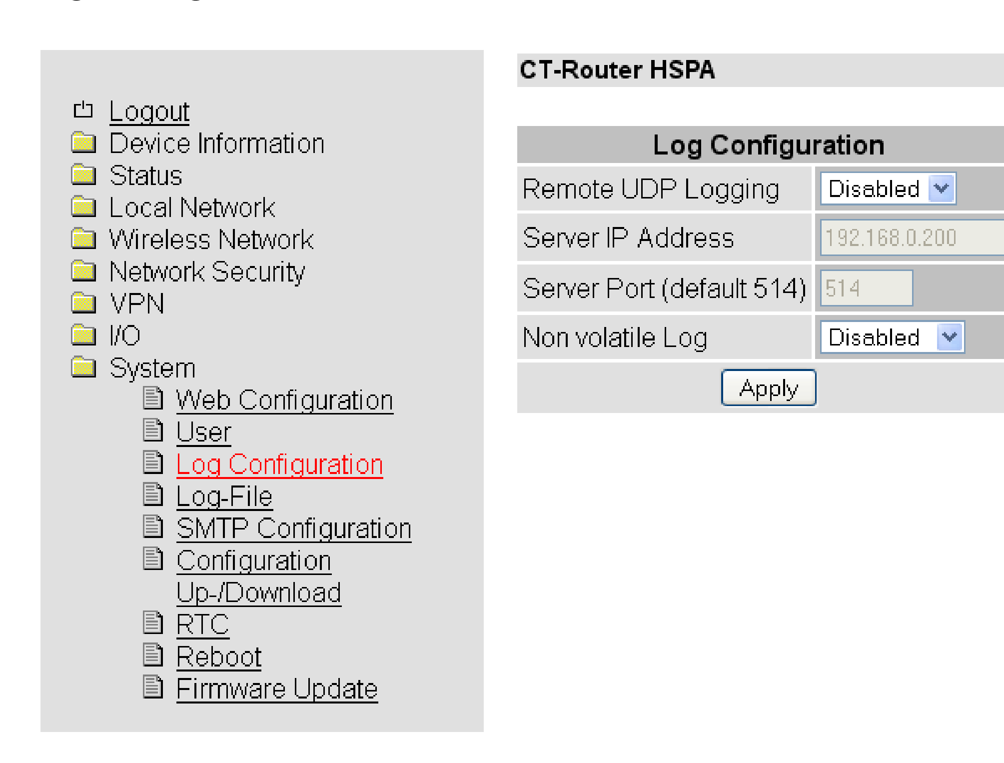
User



System >> User	
admin	Uneingeschränkter Zugriff (Schreiben und Lesen) Neues Passwort festlegen
user	Eingeschränkter Zugriff (nur Lesen / nicht alle Bereiche) Neues Passwort festlegen

System

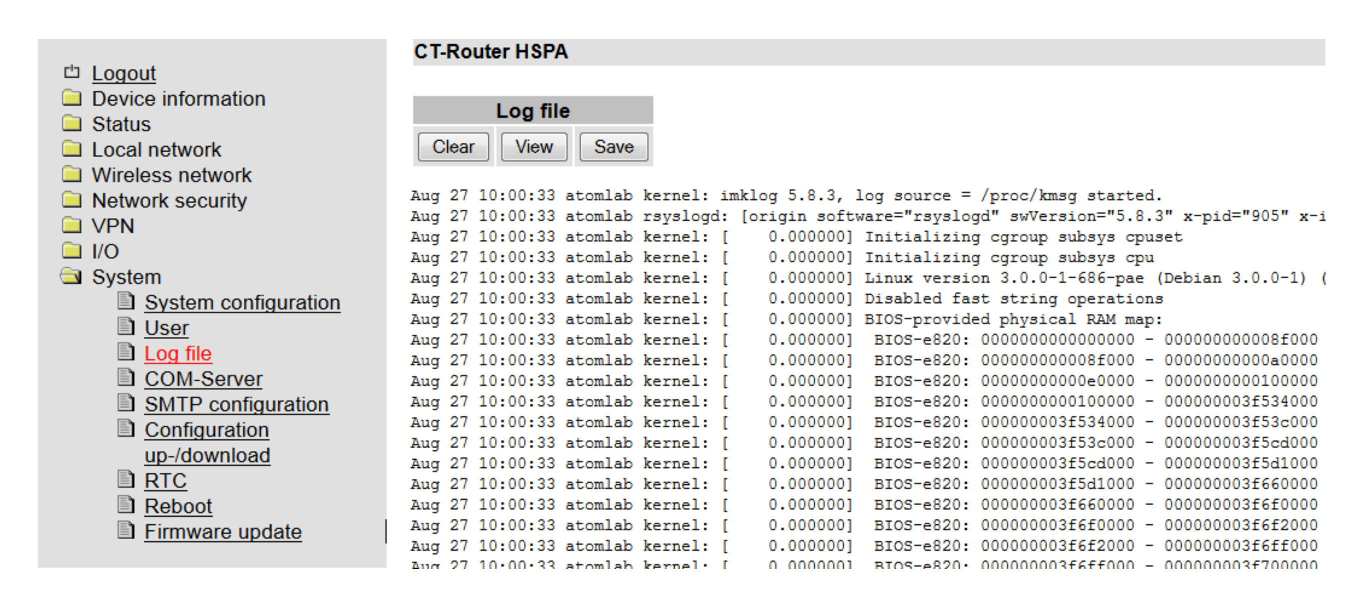
Log Configuration



System >> Log Configuration	
Remote UPD Logging	**Disabled:** Externes Logging deaktiviert **Enabled:** Externes Logging aktiviert
Server IP Address	IP-Adresse vom externen Log-Server
Server Port (default 514)	Port vom externen Log-Server
Non volatile Log	**Disable:** Speichert das Log intern auf einem vorher festgelegten Server. **USB-Stick:** Speichert das Log auf einem USB-Stick. Der USB-Stick muss am Router angeschlossen werden! **SD-Card:** Speichert das Log auf einer SD-Karte.

System

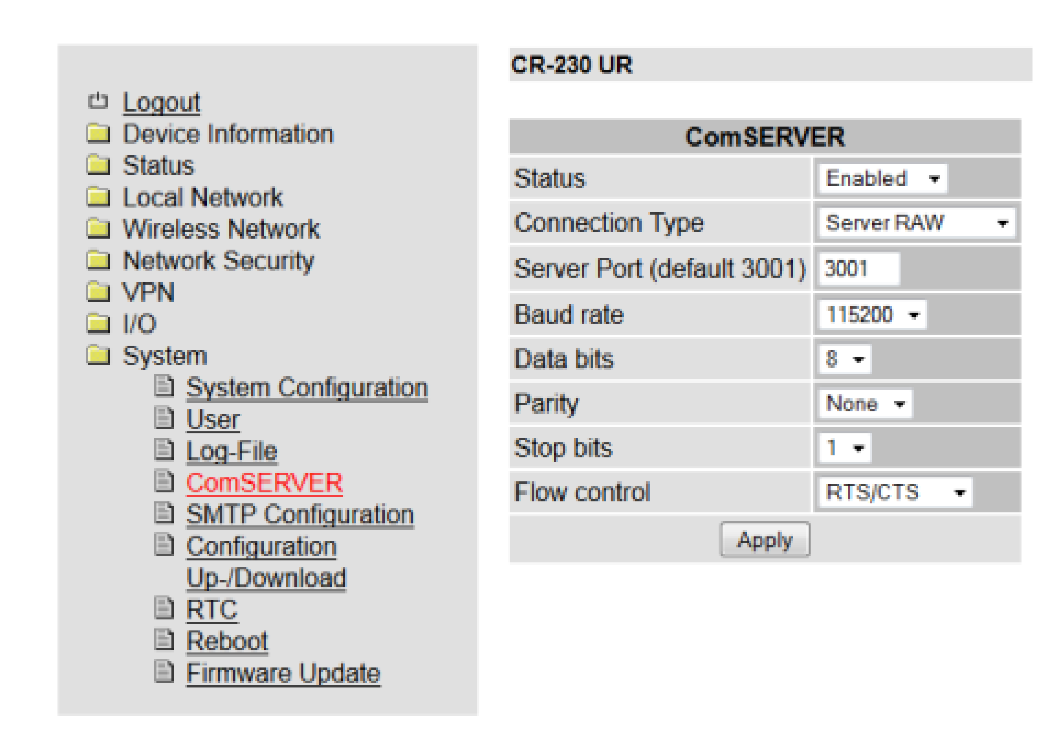
Log-File



System >> Log-File	
Clear	Einträge im internen Log-File werden gelöscht
View	Log-File Einträge werden im Browser-Fenster angezeigt
Save	Log-File wird gespeichert

System

ComSERVER - Serielle Schnittstelle konfigurieren (optional)



System >>ComSERVER	
Satus	Schnittstelle: Disabled / Enabled
Connection Type	Einstellen der seriellen Verbindung – RAW oder RFC2217
Server Port (default 3001)	Auswahl des Ports für die Netzwerkkommunikation
Baud Rate	300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
Data bits	Datenformat einstellen: Wählen Sie die Einstellungen für Datenbits, Parität und Stoppbits
Parity	
Stop bits	
Flow control	Art der Flusskontrolle auswählen

Zusammenfassung der Übertragungsparameter:

Baudrate:	110, 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200
Anzahl der Datenbits:	7 oder 8
Anzahl der Stopbits:	1 oder 2
Parität:	none, even, odd,
Flusssteuerung:	RTS/CTS, XON/XOF, RS485 RTS oder keine

System

SMTP Configuration

Logout
Device Information
Status
Local Network
Wireless Network
Network Security
VPN
I/O
System
Web Configuration
User
Log Configuration
Log-File
SMTP Configuration
Configuration Up-/Download
RTC
Reboot
Firmware Update

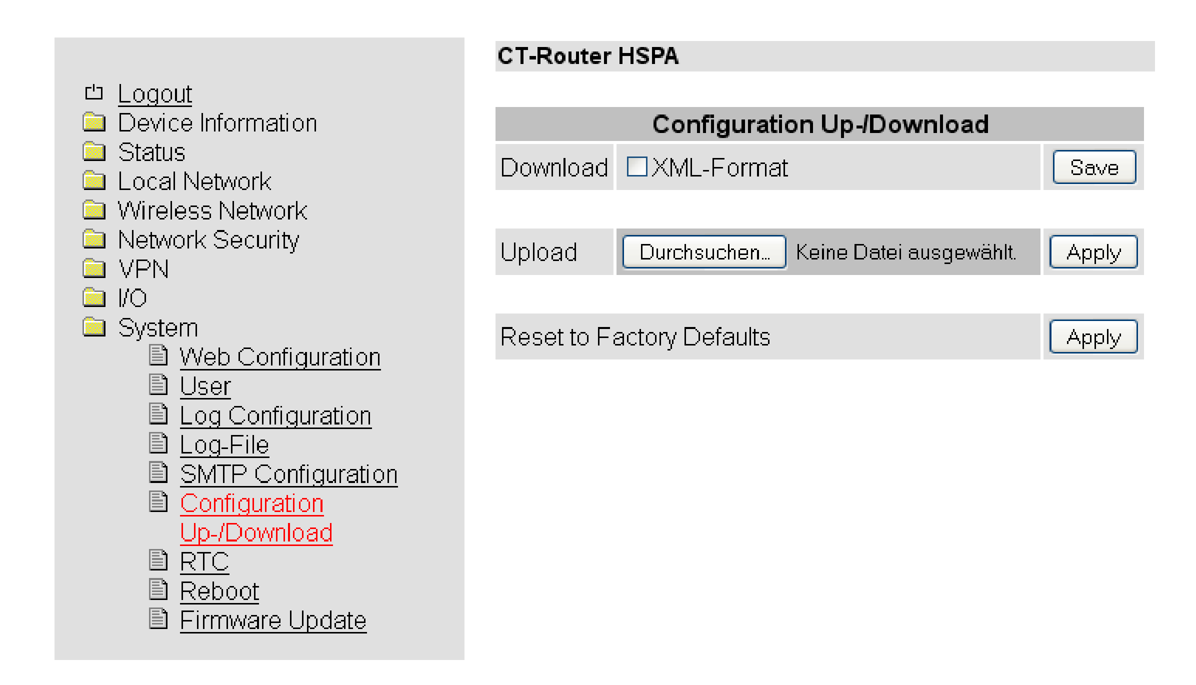
CT-Router HSPA

SMTP Configuration	
SMTP Server	
Server Port (default 25)	25
Transport Layer Security	None
Authentication	Plain Password
Username	
Password	
From	
Apply	

System >>SMTP Configuration	
SMTP Server	IP-Adresse / Hostname des SMTP Servers
SMTP Port (default 25)	Port des SMTP Servers
Transport Layer Security	Verschlüsselung: Keine, STARTTLS, SSL/TLS
Authentication	No authentication: Keine Authentifizierung Plain Password: Authentifizierung Benutzername und Passwort (unverschlüsselte Übertragung der Authentifizierungsdaten). Encrypted Password: Authentifizierung mit Benutzername und Passwort (verschlüsselte Übertragung der Authentifizierungsdaten)
Username	Benutzername
Password	Passwort
From	Absender der Mail

System

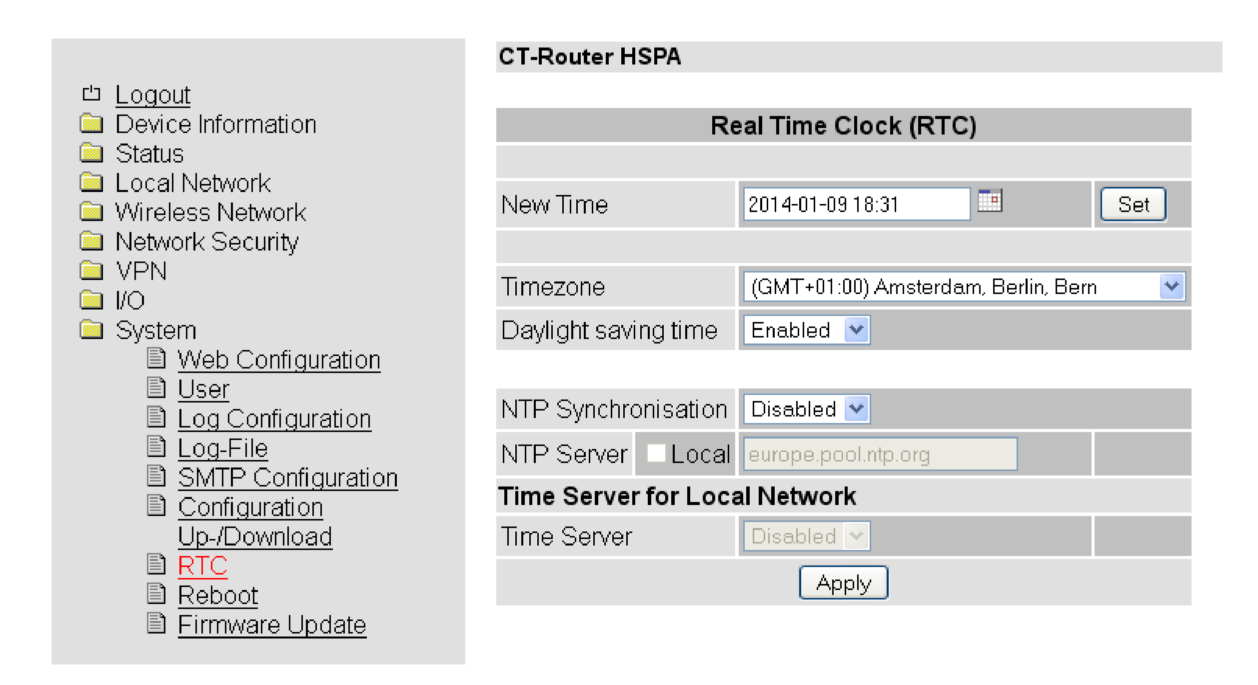
Configuration Up-/Download



System >> Configuration Up-/Download	
Download	Aktuelle Konfigurationen herunterladen
Upload	Gesicherte oder veränderte Konfigurationen hochladen und mit "apply" bestätigen.
Reset to Factory Defaults	Konfigurationen und IP-Einstellungen auf Werkeinstellung zurücksetzen. Hochgeladene Zertifikate bleiben erhalten.

System

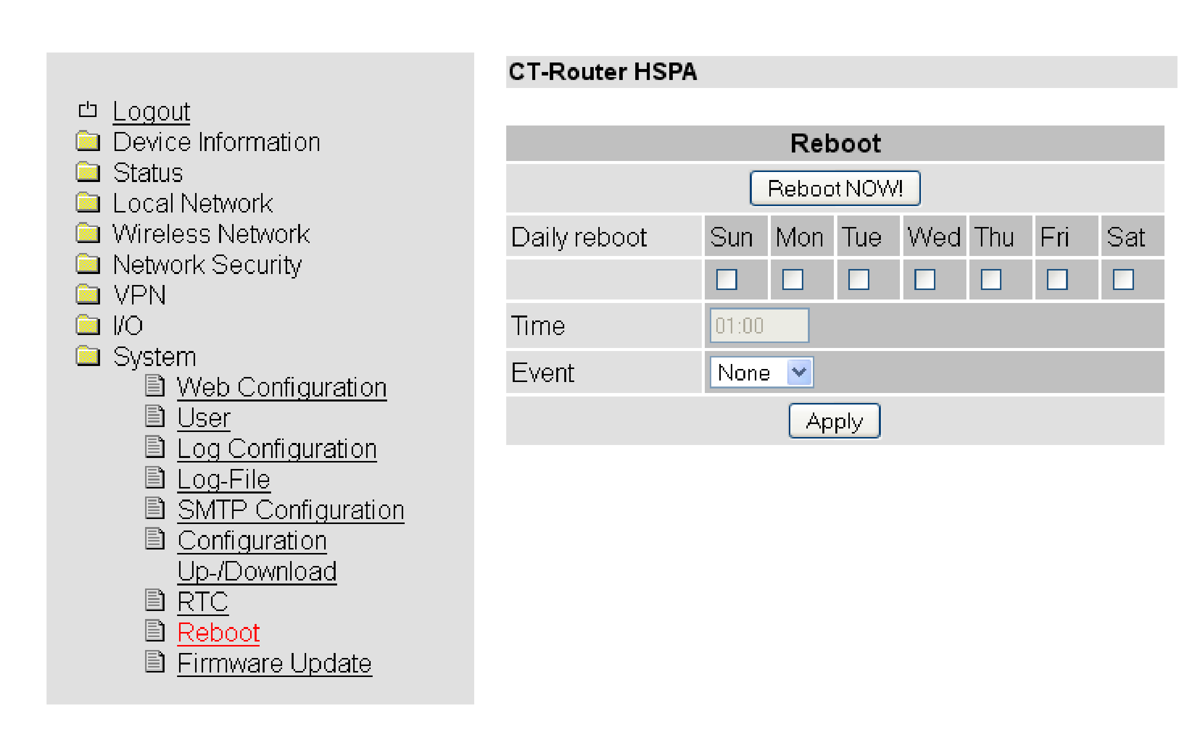
RTC



System >> RTC	
New Time	Manuelle Zeitkonfiguration, falls kein NTP-Server vorhanden ist.
Timezone	Zeitzonenauswahl
Daylight saving time	**Disable:** Sommerzeitberücksichtigung deaktiviert **Enable:** Sommerzeitberücksichtigung aktiviert
NTP Synchronisation	Datum und Uhrzeit können mit einem NTP-Server synchronisiert werden. Bei Erstverwendung dieser Funktion kann die erste Synchronisation bis zu 15 Minuten dauern.
NTP Server	Im LAN-Netzwerk kann der Router als NTP-Server eingestellt werden. Es wird hierzu eine Adresse von einem NTP-Server benötigt. Die NTP Synchronisation muss auf Enable gestellt werden.
Time Server	**Disable:** Zeitserverfunktion für das lokale Netzwerk deaktiviert **Enable:** Zeitserverfunktion für das lokale Netzwerk aktiviert

System

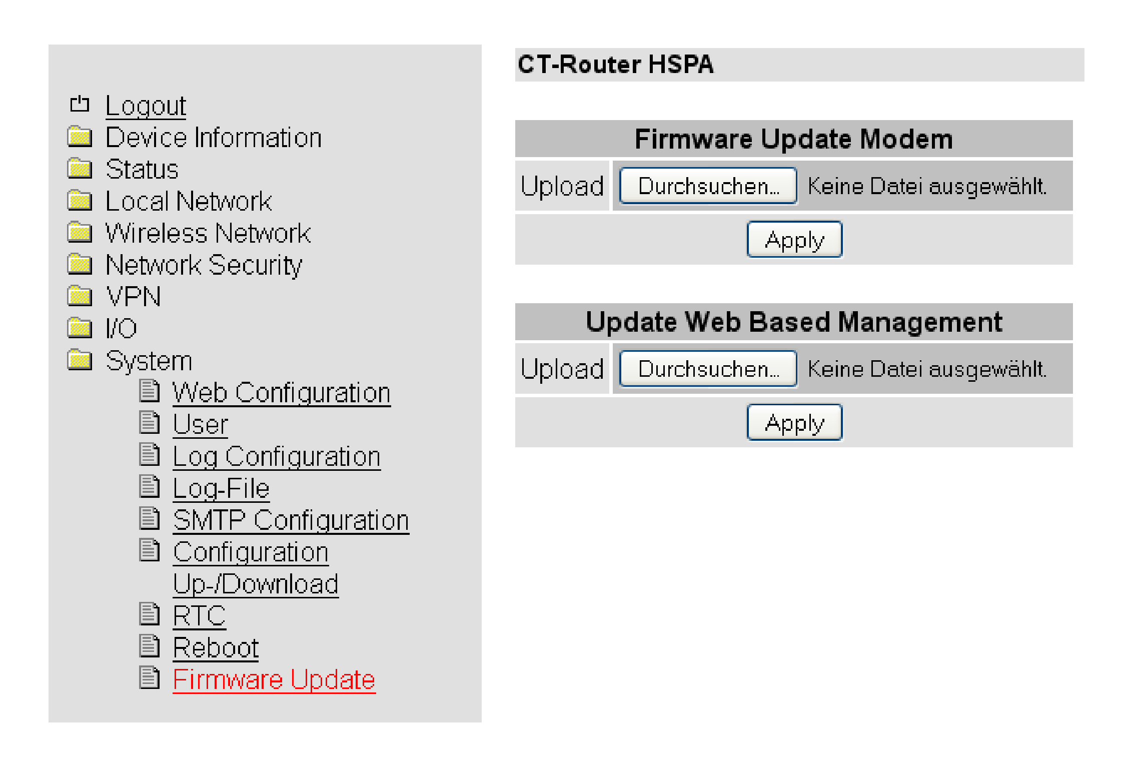
Reboot



System >> Reboot	
Reboot NOW!	Sofortigen Neustart des Routers erzwingen!
Daily reboot	Den Router an bestimmten Wochentagen zum bestimmten Zeitpunkt neustarten. Mit Klicken auf die Kontrollkästchen legen Sie die Wochentage für den Neustart fest.
Time	Uhrzeit des Neustarts (Stunde:Minute)
Event	Router kann mit digitalem Eingang neugestartet werden. Signal sollte nach einem Neustart wieder "Low" sein.

System

Firmware Update



System >> Firmware Update	
Firmware Update Modem	Diese Updates sorgen für Funktionserweiterungen und Produktaktualisierungen.
Update Web Based Management	Diese Updates beziehen sich auf die Konfiguration über einen Internetbrowser.

Abfrage und Steuerung über XML Dateien

Format der XML Dateien

Jede Datei beginnt mit dem Header:
<?xml version="1.0"?>
oder
<?xml version="1.0" encoding="UTF-8"?>

Gefolgt von dem Basis-Eintrag. Folgende Basis-Einträge stehen zur Auswahl:

<io>	*</io>*	# E/A-System
<info>	*</info>*	# Allgemeine Informationen abfragen
<cmgr ...>	*</cmgr>*	# SMS versenden (nur Mobilfunkgeräte)
<email ...>	*</email>*	# eMail versenden

Alle Daten werden in UTF-8 kodiert. Folgende Zeichen müssen
als Sequenzen übertragen werden:
& - &
< - <
> - >
" - "
' - '

Beispiele zu den Basis-Einträgen:

a) E/A System

```
<?xml version="1.0"?>
<io>
<output no="1"/>                  # Zustand von Ausgang 1 abfragen
<output no="2" value="on"/>       # Ausgang 2 einschalten
<input no="1"/>                   # Zustand von Eingang 1 abfragen
</io>
```

Hinweis: Als "value" kann sowohl on/off als auch 0/1 angegeben werden.
Zurückgegeben wird immer on oder off.

Zurückgeliefert wird etwa folgendes:

```
<?xml version="1.0" encoding="UTF-8"?>
<result>
<io>
<output no="1" value="off"/>      # Zustand von Ausgang 1; hier eingeschaltet
<output no="2" value="on"/>       # Zustand von Ausgang 2; wurde eingeschaltet
<input no="1" value="off"/>       # Zustand von Eingang 1; hier ausgeschaltet
</io>
</result>
```

Zu beachten ist, das Ausgänge, welche ferngesteuert werden sollen, als"Remote Controlled" konfiguriert sein müssen

Abfrage und Steuerung über XML Dateien

b) Allgemeine Informationen abfragen

```
<?xml version="1.0"?>
<info>
<device />                # Gerätedaten abfragen
<radio />                 # Daten zur Funkverbindung abfragen (nur Mobilfunkgeräte)
</info>
```

Zurückgeliefert wird etwa folgendes:

```
<?xml version="1.0" encoding="UTF-8"?>
<result>
<info>
<device>
<serialno>13120004</serialno>
<hardware>A</hardware>
<firmware>1.00.4-beta</firmware>
<wbm>1.34.8</wbm>
<imei>359628040604790</imei>
</device>
<radio>
<provider>Vodafone.de</provider>
<rssi>15</rssi>
<creg>1</creg>
<lac>0579</lac>
<ci>26330CD</ci>
<packet>0</packet>
</radio>
</info>
</result>
```

c) SMS versenden

```
<?xml version="1.0"?>
<cmgs destaddr="0123456789">Dies ist der SMS-Text</cmgs>
```

Zurückgeliefert wird etwa folgendes:

```
<?xml version="1.0" encoding="UTF-8"?>
<result>
<cmgs length="98">SMS accepted</cmgs>
</result>
```

d) eMail versenden

```
<?xml version="1.0"?>
<email to="x.yz@diesunddas.de" cc="info@andere.de">
<subject>Test Mail</subject>
<body>
    Dies ist ein mehrzeiliger eMail-Text.
    mfg. ihr Router
</body>
</email>
```

Abfrage und Steuerung über XML Dateien

Zurückgeliefert wird etwa folgendes:


```
<?xml version="1.0" encoding="UTF-8"?>
<result>
<email>done</email>
</result>
```


oder im Fehlerfall:


```
<?xml version="1.0" encoding="UTF-8"?>
<result>
<email error="3">transmisson failed</email>
</result>
```


Hinweis zur Darstellung: die Einrückungen und Zeilenumbrüche dienen nur der Verständlichkeit und müssen so nicht gesendet werden, noch werden sie so gesendet. Alle empfangenen Daten sollten mit einem XML-Parser wie z.B. Expat interpretiert werden.

Daten senden und empfangen

Der Kommunikationsablauf ist folgender:

- Verbindung zum Socket-Server aufbauen
- Daten senden
- Zurückgegebene Daten mit XML-Parser interpretieren
- Verbindung schließen

Funktions-Test

Funktions-Test mittels Windows Hyperterminal

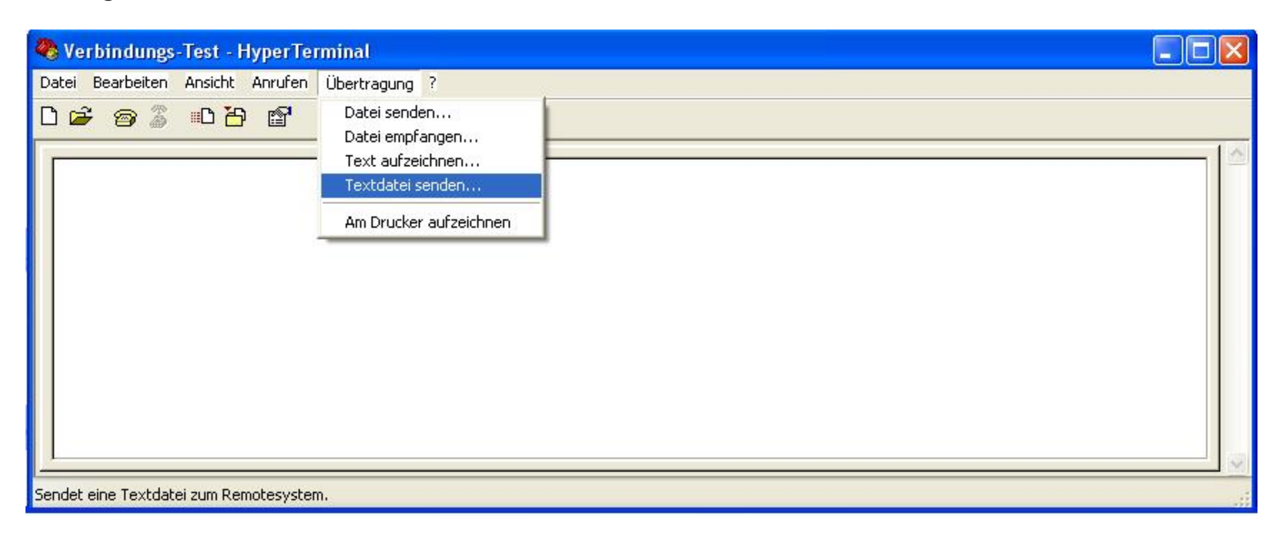
Für einen Test kann unter Windows das bekannte Programm „Hyperterminal" verwendet werden. Über Hyperterminal können XML-Dateien an den Socket Server des Routers gesendet werden. Die entsprechenden XML-Dateien (siehe Kapitel „Abfrage und Steuerung über XML Dateien") müssen dafür vorab auf Ihren Bediener-PC gespeichert worden sein. Öffnen Sie Hyperterminal und konfigurieren Sie die gewünschte Verbindung (Hier ein Beispiel unter der Verwendung von Default-Einstellungen):

Hostadresse:	192.168.0.1 (IP-Adresse des Routers / Socket Servers)
Anschlussnummer:	1432 (Port des Socket Servers)
Verbindung herstellen über:	TCP/IP (Winsock)





Öffnen Sie die Verbindung und wählen Sie im Menü von Hyperterminal „Übertragung / Textdatei senden...." die zu übertragende XML-Datei aus.



Nach der erfolgreichen Übertragung erhalten Sie die Antwort auf Ihre Anfrage.

Applikationsbeispiele

Eine Verbindung zum Internet herstellen

Mit dem IKOM-ROUTER haben Sie via Mobilfunknetz den Zugang zum Internet.
Es wird eine SIM-Karte eines Mobilfunkanbieters benötigt, die für Paketdaten-Dienste, zum Beispiel GPRS/EDGE oder UMTS/HSPDA, freigeschaltet ist.

Der IKOM-ROUTER ist bei dieser Applikation:

- Router
- Default Gateway
- DNS-Server
- Firewall

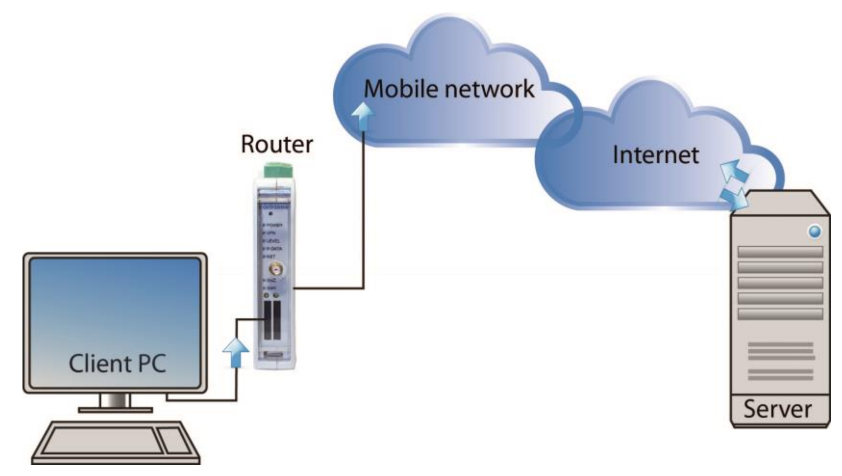
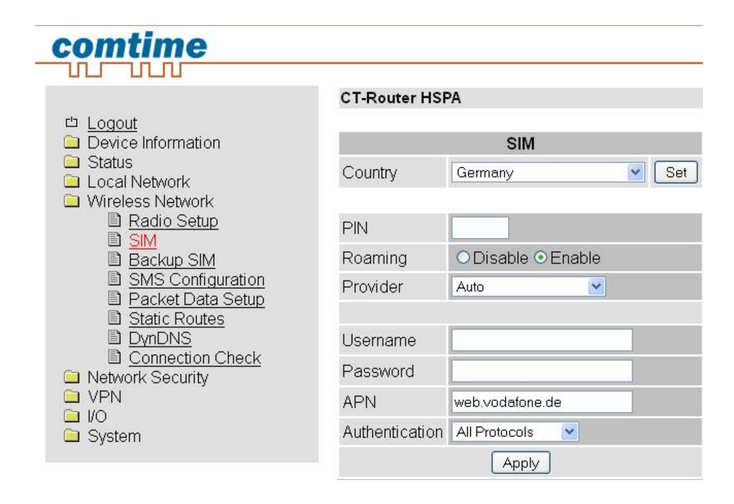


Bild: Zugang zum Internet

Vor dem Start prüfen Sie ob ausreichende Netzabdeckung durch Ihren Provider zur Verfügung steht, nur dann können Datenverbindungen aufgebaut werden.

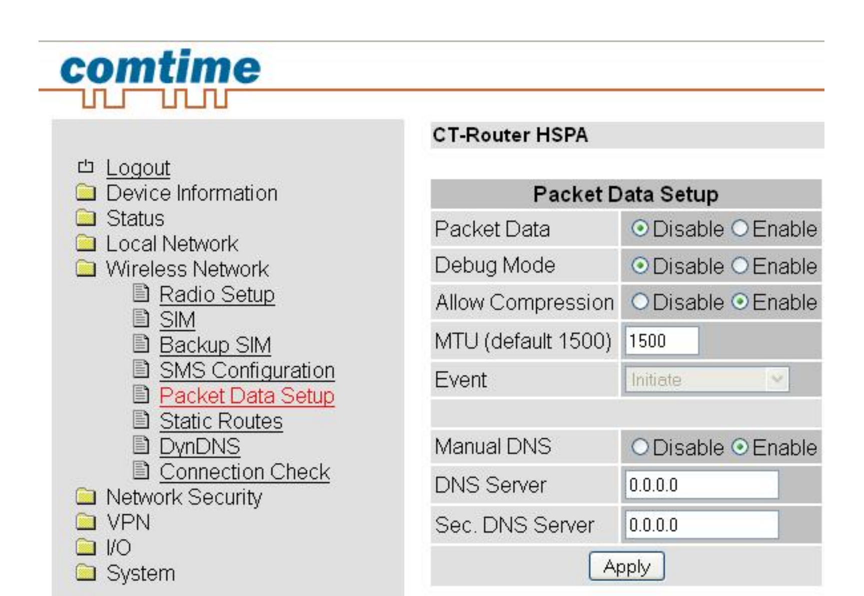
ROUTER konfigurieren:

- Öffnen Sie auf dem PC einen Browser.
- IP-Adresse im Adressfeld des Browsers eingeben (default 192.168.0.1)
- Benutzername und Kennwort eingeben (Default: Benutzername „admin" und Kennwort „admin")
- Öffnen Sie „Wireless Network“ und „SIM" und tragen Sie in das Feld „PIN" die PIN-Nummer der SIM-Karte ein. Tragen Sie zusätzlich die Zugangsdaten, APN, Username und Password für die Paketdatenübertragung in Ihrem Mobilfunknetz ein. Die Zugangsdaten erhalten Sie von Ihrem Mobilfunkanbieter.



Applikationsbeispiel

- Wechseln Sie zu „Wireless Network“ und „Packed Data Setup“ und aktivieren Sie die Paketdatenübertragung im Mobilfunknetz.
  Setzen Sie dazu „Packet Data" auf „Enable".



- Damit Sie von Ihrem PC ins Internet gelangen, müssen Sie in den Netzwerkeinstellungen die IP-Adresse des Routers als Default-Gateway und als DNS-Server eintragen.
  Die Einstellungen für Ihr Betriebssystem finden Sie in der entsprechenden Dokumentation

